Invitation to Bid: Appointment of a Service Provider for Outsourcing of ICT Services as a Single Service Aggregator including Network Services and Infrastructure

Bid Number	GNP-099-25
Advert Date	01 December 2025
Issuer	South African National Parks
Closing Date and Time	**22 January 2026 at 11H00**

TABLE OF CONTENTS

1 INTRODUCTION TO SANPARKS

As a leading conservation authority, SANParks is a public entity under the jurisdiction of the Department of Forestry, Fisheries and the Environment (DFFE), where inclusive conservation as opposed to previous policies of exclusion is central to advancing the policies in line with the National Development Framework for Sustainable Development and the National Development Plan.

South Africa's national parks conserve the country's rich diversity of flora and fauna through a system of 21 national parks, including three world heritage sites and ten marine protected areas (in terms of the National Environmental Management: Protected Areas Act No. 57 of 2003). This represents approximately 70% of state-owned terrestrial protected areas and 22% of state-managed marine protected areas, comprising over four million hectares (ha) on land and almost 370 000 ha at sea. In addition, five parks are integral components of Transfrontier conservation areas with Namibia, Botswana, Zimbabwe, Mozambique, and Lesotho.

A key intrinsic value consideration for national parks and marine protected areas as public-good is their promotion of shared natural and cultural heritages as well as their contribution to building national solidarity and pride. Located largely in rural areas, they are catalysts for economic growth which can create employment and transformation in areas that generally lack such opportunities. They also contribute significantly to the preservation of water resources, protect the archaeological and historical record, and safeguard endangered ways of life.

The National Environmental Management Protected Areas Act mandates SANParks to create destinations for nature-based tourism in a manner that is not harmful to the environment. SANParks generates a substantial percentage of its operating budget from its ecotourism business, therefore, the fulfilment of its conservation mandate is heavily reliant on thriving and sustainable tourism operations.

Legislative and Constitutional Mandate

SANParks was initially established in terms of the now repealed National Parks Act, 57 of 1976 and continues to exist in terms of the National Environmental Management: Protected Areas Act, 57 of 2003, with the mandate to conserve, protect, control and manage national parks and other defined protected areas and their biological diversity (biodiversity). As a public entity, SANParks is also governed by the Public Finance Management Act, Act 1 of 1999 (as amended by Act 29 of 1999) and is listed as a Schedule 3 Part A: 25 public entity.

SANParks delivers a diverse and complex public good mandate* that includes management of biodiversity and cultural heritage, the sustainable use of biological resources, socio-economic development, protection of ecological infrastructure, access to nature, science, educational and cultural experiences and reconnecting and inspiring people.

Section 24(b) of the Constitution of the Republic of South Africa, 1996 underpins the SANParks mandate, which states that everyone has the right to:

- an environment that is not harmful to their health or well-being; and
- have the environment protected for the benefit of present and future generations through reasonable legislative and other measures that:

- prevent pollution and ecological degradation;
- promote conservation; and
- secure ecologically sustainable development and use of natural resources, while promoting justifiable economic and social development.

The parks under the management of SANParks are divided into 6 regions:

Region	Regional Office	Parks managed
Arid	Upington	Kgalagadi, Augrabies, Richtersveld, Namaqua, Mokala, Meerkat
Cape	Cape Town	Table Mountain, Agulhas, West Coast, Tankwa Karoo, Bontebok
Garden Route	Knysna	Storms river Mouth (Tsitsikamma), Knysna Forests, Wilderness, Knysna Estuary
Frontier	Port Elizabeth	Addo, Camdeboo, Mountain Zebra, Karoo
North	Pretoria, Head Office	Golden Gate, Marakele, Mapungubwe
Kruger National Park	Skukuza	35 Various Camps
Administrative	N/A	Groenkloof (Head Office)

Furthermore, SANParks oversees the management of the Parks and provide strategic guidance and support from its Head Office in Pretoria.

2 CONTEXT OF THIS PROCUREMENT

South African National Parks (SANParks) invites Bidders to submit proposals for appointment as the Single Service Aggregator (SSA) for SANParks for a period of **ten (10) years**. Over this extended period, the successful Bidder will be entrusted with supporting, enabling, and advancing SANParks' management objectives and ICT requirements, ensuring that its technology environment evolves in step with the rapid pace of change in the global and South African ICT landscape.

Given the strategic importance and duration of this engagement, it is an important factor that Bidders demonstrate innovation, foresight, and a plan for keeping SANParks at the forefront of technology. This should include how emerging technologies will be assessed and if needed integrated when agreed to, and how the organisation's ICT environment will be kept agile, secure, and fit for purpose throughout the contract period.

Based on the information contained in responses to this document, SANParks will enter negotiations with the successful Bidder for the purposes of concluding a binding contract, inclusive of supporting services and associated Service Level Agreements.

An SSA is required to deliver and manage all necessary ICT services. While SANParks may have existing agreements in place for certain products and services which will be detailed below, the successful Bidder will be expected to manage these agreements and concurrently design and

implement a new, fit-for-purpose service model. This may include subcontracting to specialist service providers where appropriate, but ultimate accountability will rest with the appointed Bidder.

The model proposed is based on Service Integration and Management (SIAM) an approach to managing multiple suppliers of both business and information technology services, integrating them into a single business facing IT organisation. SIAM aims to seamlessly combine interdependent services from various internal and external providers into cohesive, end-to-end services aligned with our business requirements.

Bidders' responses will be evaluated on their approach to delivering the key IT capabilities, addressing the challenges, and achieving the benefits defined in the SIAM model.

3 BUSINESS UNIT RESPONSIBLE

The Information and Communications Technology Operations (ICTO) department of SANParks is responsible for managing and maintaining the organisation's technology infrastructure, including hardware, software, networking, and telecommunications systems. These responsibilities are delivered through two operational units which are: Information Technology Operations (IT OPS) and Enterprise Applications Development (EAD).

The IT Operations focuses on the infrastructure components such as the management of networks, servers, security, and telecommunications systems. The Enterprise Applications Development unit focuses on the development and management of business systems (Finance, SCM, HCM, ECM, Tourism, e-commerce/website etc.), software quality assurance and technical support.

The appointment of a service provider for the development, maintenance, and support of the OpenText app works environment will be managed by the Enterprise Applications Development unit of the ICTO department.

Please note that the following applications are in use by SANParks and are managed by third parties. This table is presented to make the Bidder aware of these services, but the Bidder does not need to manage these applications:

Applications Managed by Third Parties
MS Dynamics GP – Great Plains
Panorama Necto
Power BI
Rubrik
Microsoft Dynamics CRM Loyalty Management Application
Microsoft Enterprise Agreement
Online Payment Gateway
Business Process Management Application
RoomSeeker / Plankton

Applications Managed by Third Parties
Sage VIP Payroll and Premier HR
Memex
SANParks Reservation System (will replace RoomSeeker)
NAC-Forescout
BizAzure Integration Services
Proofpoint- Security Awareness

4 DISCLAIMERS

SANParks has produced this document in good faith. SANParks, its agents, employees, and associates do not warrant its accuracy or completeness. To the extent that SANParks is permitted by law, SANParks will not be liable for any claim whatsoever and howsoever arising (including, without limitation, any claim in contract, negligence or otherwise) for any incorrect or misleading information contained in this document due to any misinterpretation of this document. SANParks makes no representation, warranty, assurance, guarantee, or endorsements to any provider/Bidder concerning the document, whether regarding its accuracy, completeness or otherwise, and SANParks shall have no liability towards the responding service providers or any other party in connection therewith.

NB: Important Notice: ***Bidders must be aware of scammers who pose as SANParks employees selling bid documents or offering monetary gratuity in exchange for information or awarding of bids.***

All documents shall be found on the SANParks website and eTender Portal and awarded bids are notified through the website under "bids awarded". SANParks shall never ask any Bidder for monetary gratuity in exchange for information or manipulating outcome of bids**.**

5 THE BIDDING SELECTION PROCESS

The evaluation process will be conducted in various phases. To move to the next phase of evaluation, the previous phase of evaluation must have been fully complied with. No leniency for non-submitted documents / proof or late submission will be allowed. If your response is incomplete, your bid will be disqualified and will NOT progress to the next phase.

The bid evaluation phases are as follows:

- **Phase 1 – Mandatory Evaluation Phase:**

  This phase verifies that all mandatory requirements are met.

- **Phase 2 – Technical/Functionality Evaluation Phase:**

This phase evaluates the bid responses in line with the evaluation criteria detailed under paragraph "Technical / Functionality evaluation. Bidders must achieve a minimum score of 75% in this phase for their bid to progress to the next phase of evaluation.

- **Phase 3 – Price and Preference Evaluation Phase (specific goals):**

  This phase evaluates and scores the commercial aspects of the bid and the specific goals will be evaluated and scored according to the methodology described in our Supply Chain Management forms, (SBD FORMS), attached to this bid.

Based on the above outcome of the bid evaluation phases, the Bid Evaluation Committee will make recommendations to the Bid Adjudication Committee for recommendation of award of the bid.

Due to the expected contract value and duration, the Board of SANParks will be the final approval authority.

Thereafter, a Single Service Aggregator Agreement will be drafted to be signed by both parties.

- **Phase 1: Mandatory Evaluation Criteria**

  It is essential for all Bidders to note that the process of evaluation will be done in phases. In this phase potential Bidders will be evaluated to ensure that they comply with the mandatory criteria.

  Failure to comply with any of the Mandatory Requirements will lead to the Bidder being disqualified and not considered for further evaluation. Only Bidders who can provide acceptable documentary proof that complies with the following mandatory criteria will be considered for the next phase of evaluation.

  The Bidder must—

  (1) Hold the following licences from ICASA—

  a. Electronic Communications Services Licence (ECS).

  b. Electronic Communications Network Services Licence (ECNS).

  Copies of both licences must be provided. Bidders must submit their bids in the name of the ECS and ECNS license holder who will be the prime contracting party. Bids that are not submitted in the name of the ECS and ECNS license holder will be disqualified.

  (2) Provide a signed letter of financial backing from an authorised financial institution to the value of 10% or more of the total bid value in relation to this bid.

  (3) Hold the Microsoft Solutions Partner designations in Modern Work and Security as mandatory requirements. Proof of Evidence from Microsoft showing the Modern Work and Security is required.

  (4) Without any prejudice to any terms that may be agreed under any Single Service Aggregator Agreement, provide proof of adequate insurance (a letter from the applicable insurer or broker), which at a minimum should include—

a. insurance in terms of the Compensation for Occupational Injuries and Diseases Act, 1993 or other relevant legislation ("**COIDA**"); and

b. proof of the Bidder's professional indemnity insurance in line with the nature of services to be rendered under this Invitation to Bid.

All above letters must be valid at the time of the bid closure.

(5) Provide proof of data centre operations within the boundaries of South Africa, as follows—

a. proof of data centre operations (for two data centres – production and disaster recovery) by way of a valid Uptime Institute certificates showing the operation of a Tier III/IV data centre OR a binding partnership agreement with a Tier III/IV data centre who holds an Uptime Institute certificate. Please note that the Bidder must provide both certificates for production and disaster recovery sites; and

b. all the certificates must be valid at the time of the bid closure.

(6) Provide the following minimum and valid certifications—

a. ISO 9001 – Quality Management Systems;

b. ISO 20000-1 – Service Management;

c. ISO 27001 – Information Security Management;

d. ISO 27017 – Information Security for Cloud Services Guidance;

e. ISO 27018 – Protection of Personally Identifiable Information (PII) in Public Clouds; and

f. SOC 2 Type II / ISAE 3000.

All certificates must be valid at the time of the bid closure. Certificates under application or noted as “in progress” will not be accepted.

The Bidder will only progress to Phase 2 if all the mandatory criteria above have been met.

- **<u>Phase 2: Technical/Functional Evaluation Criteria</u>**

In this phase, all bids that have met the mandatory requirements outlined above will be evaluated as follows—

(1) Technical/Functional Evaluation threshold: Bidders must achieve an overall score of at least 75% based on the criteria below to be considered for the next phase. Bidders who do not meet the minimum technical threshold of 75% will be disqualified.

(2) Several functionality criteria set out below require substantiated evidence of compliance as set out below.

FUNCTIONALITY CRITERIA	WEIGHTING (%)	MAXIMUM TO BE AWARDED
Ability to provide the services by Field Service Engineers (FSEs) at all the identified sites Given SANParks' large geographic distribution over South Africa, the Bidder must be able to demonstrate their ability to support the various SANParks sites. This may require the Bidder's own staff providing the support or a combination where certain services are sub-contracted to other service providers under the direct management of the Bidder. Scoring will be awarded using the average number of hours across all the sites. Please use **Annexure 1E** of the GNP-099-25 Annexures Excel Spreadsheet to capture the locations of FSEs. Please note that incomplete spreadsheets will lead to zero points being allocated.	**20**	20 = Support engineers less than 1 hour from site. 16 = Support engineers from 1 hour but less than 2 hours from site. 12 = Support engineers from 2 but less than 4 hours from site. 8 = Support engineers from 4 hours but less than 6 hours from site. 4 = Support engineers from 6 hours but less than 8 hours from site. 0 = Support engineers 8 or more hours.
Managed Services Experience Please provide evidence of experience in managing services, associated contracts and vendors. Please provide the references on the client's letterheads, with the following information included: • name of the official and signature as well as position and email address; • client's official contact number; • the specific services provided to the client; and • start and end dates of the services that were provided to the client. The services must be for Managed Services in South Africa within the past five (5) years. This must be indicated in the body of the reference letter.	**10**	5 = Experience has been shown in all 5 of the managed services. 0 = Experience has not been demonstrated in all 5 of the managed services. If 0 points has been allocated above, then no points will be allocated for experience. Where 5 points has been allocated for the above, points for experience will be evaluated and allocated as follows: 5 = Average of 5 years or more experience across all managed services. 4 = Average of at least 4 years' experience but less than 5 years' experience across all managed services. 3 = Average of at least 3 years' experience but less than 4 years' experience across all managed services.

FUNCTIONALITY CRITERIA	WEIGHTING (%)	MAXIMUM TO BE AWARDED
Please cover the following managed services at a minimum: • Front Office Services; • Back Office Services; • End User Services; • ISP/Connectivity Services; and • Data Centre Management. If any of the above information is missing, the reference letter will not be considered.		2 = Average of at least 2 years' experience but less than 1 years' experience across all managed services. 1 = Less than 1 year of experience. 0 = No evidence of experience provided.
Capability The Bidder must provide the resource, with their relevant experience, certifications and qualifications as per **Annexure 1G** of the GNP-099-25 Annexures Excel Spreadsheet. Bidders must also provide copies of CV's as well as all relevant certificates and qualifications. Any CV that is not accompanied by the relevant certification, will score 0.	**35**	35 points will be allocated if the average score equals or exceeds 80%. 25 points will be allocated if the average score is between 70% and 79%. 0 Points will be allocated if the average score is less than 70%. Note: The % is an average of all scores entered across all required capabilities listed in Annexure 1G of the GNP-099-25 Annexures Spreadsheet.
Experience in the Management of Endpoints Bidders must provide relevant evidence of experience in managing endpoints. Acceptable evidence includes either official client letters or a letter from the OEM.	**5**	5 = ≥ 40000 endpoints managed. 4 = < 40000 and ≥ 30000 endpoints managed. 3 = < 30000 and ≥ 20000 endpoints managed. 2 = < 20000 and ≥ 10000 endpoints managed. 1 = < 10000 endpoints managed. 0 = Bidder's endpoint managed capability does not exist.

FUNCTIONALITY CRITERIA	WEIGHTING (%)	MAXIMUM TO BE AWARDED
Experience in the Management of Servers Bidders must provide relevant evidence of experience in managing servers. Acceptable evidence includes either official client letters or a letter from the OEM.	**5**	5 = ≥ 4000 servers managed. 4 = < 4000 and ≥ 3000 servers managed. 3 = < 3000 and ≥ 2000 servers managed. 2 = < 2000 and ≥ 1000 servers managed. 1 = < 1000 servers managed. 0 = Bidder's server management capability does not exist.
Experience in the Management of Databases Bidders must provide relevant evidence of experience in managing databases. Acceptable evidence includes either official client letters or a letter from the OEM.	**5**	5 = ≥ 2000 databases managed. 4 = < 2000 and ≥ 1000 databases managed. 3 = < 1000 and ≥ 500 databases managed. 2 = < 500 and ≥ 250 databases managed. 1 = < 250 databases managed. 0 = Bidder's database management capability does not exist.
Experience in Disaster Recovery as a Service (DRaaS) Bidders must provide relevant evidence of experience in DRaaS capabilities. Acceptable evidence includes either official client letters or a letter from the OEM.	**10**	10 = The DRaaS capability is ≥ 10000. 8 = The DRaaS capability is ≤ 10000. 6 = The DRaaS capability is ≤ 9000. 4 = The DRaaS capability is ≤ 8000. 2 = The DRaaS capability is ≤ 7000 but ≥ 5000 0 = Bidder's DRaaS capability does not exist.
Cloud Experience Bidders must provide relevant experience in multi-cloud interconnects across the following providers in South Africa: ○ Amazon Web Services; ○ Microsoft Azure; ○ Google Cloud; and ○ Alibaba.	**10**	10 = Experience in multi-cloud interconnects > 4 mentioned providers. 8 = Experience in multi-cloud interconnects = 4 mentioned providers. 6 = Experience in multi-cloud interconnects = 3 out of the 4 mentioned providers. 4 = Experience in multi-cloud interconnects = 2 out of the 4 mentioned providers.

FUNCTIONALITY CRITERIA	WEIGHTING (%)	MAXIMUM TO BE AWARDED
Acceptable evidence includes either official client letters or a letter from the OEM.		2 = Experience in multi-cloud interconnects = 1 out of the 4 mentioned providers. 0 = Experience in multi-cloud interconnects = 0 out of the 4 mentioned providers.

6 REASONS FOR DISQUALIFICATION

SANParks reserves the right to disqualify any Bidders who do not comply with one or more of the following bid requirements and may take place without prior notice to the Bidder:

- Bidders who submit incomplete information and documentation according to the requirements of this RFB document.
- Bidders who submit information that is fraudulent, factually untrue or inaccurate information.
- Bidders who received information not available to other potential Bidders through fraudulent means.
- Bidders who fail to comply with mandatory requirements and fail to meet the minimum of 75% for the functional/technical requirements as stipulated in the RFB document.
- Bidders who misrepresent or alter material information in whatever way or manner.
- Bidders who promise, offer, or made gifts or benefits available to any SANParks employee.
- Bidders who canvassed or lobbied in order to gain unfair advantage.
- Bidders who commit fraudulent acts; and
- Bidders who act dishonestly and/or in bad faith etc.

7 CAPABILITIES

- Front Office Services (these are client-facing or service-desk-type functions)
  - Centralised Single Point of Contact (SPOC) Service Desk Aggregator
  - User Support
  - Bulk Email Service
  - Bulk SMS Service
  - Quality Assurance (when focused on client-facing service quality)

- Back Office Services (these cover internal IT management, governance, and architecture)
  - Single Service Aggregator
  - Patch Management and Support
  - Security Operations Centre (SOC) Services
  - Vulnerability Assessment Services
  - Perimeter Protection Services
  - PCI DSS Governance and Monitoring Services
  - ICT Maturity and Innovation Services
  - IT Governance Scope of Work
  - Enterprise Architecture Services Scope of Work

- Additional Criteria to be Noted (all subsections: Geographical Capacity, Experience, Identity, Performance, Service Levels)

- End User Services (everything delivered directly to users or their devices)
  - User Support (also in Front Office, but operationally fits here too)
  - User Device Configuration
  - Mimecast Management
  - Patch Management and Support (end-user device level)

- ISP/Connectivity Services (covers WAN, LAN, internet, and telephony)
  - Local Area Network Installation and Maintenance Services
  - Wide Area Network Services
  - Internet Access Services
  - IP Telephony Services

- Data Centre Management (covers compute, storage, backup, DR, databases, and cloud)
  - Server Management
  - Database Administration
  - Disaster Recovery Management
  - Cloud Management Services

8 STRUCTURE

- Prime-Vendor Approach.

9 CONTRACT PERIOD

The contract is a for a period of ten (10) years.

10 SPECIFICATIONS/SCOPE OF WORK

SANParks is seeking the following services from a service provider built on ITIL® standards of service delivery and strictly following best practices as prescribed in CoBIT®.

As this approach is based on an SSA model, Bidders are required to clearly specify whether they will provide the service themselves or identify the sub-contractor responsible for delivering the service/s. The Bidder must perform at least 70% of the services and will retain full legal, operational, and financial responsibility for all subcontracted services.

The required services are discussed further in this document under the following headings —

10.1	**Core Services**
10.1.1	Single Service Aggregator
10.1.2	Centralised Single Point of Contact (SPOC) Service Desk Aggregator
10.1.3	User Support
10.1.4	User Device Configuration
10.1.5	Network Management (WAN, LAN and Internet)
10.1.6	Server Management
10.1.7	Database Administration

10.1.8	Disaster Recovery Management
10.1.8.1	Backup and Recovery
10.1.8.2	Supported Workloads
10.1.8.3	Storage and Archiving
10.1.8.4	Security and Compliance
10.1.8.5	Automation and Integration
10.1.8.6	Performance and Efficiency
10.1.8.7	Reporting and Alerting
10.1.8.8	Deployment Models
10.1.9	Mimecast Management
10.1.10	Patch Management and Support
10.2	**LAN/WAN**
10.2.1	Local Area Network Installation and Maintenance Services
10.2.1.1	Network Points
10.2.1.2	Expansion of the LAN
10.2.2	Wide Area Network Services
10.2.2.1	Wide Area Network Requirements
10.2.2.2	Internet Access Services
10.2.2.3	IP Telephony Services
10.2.2.3.1	General Business Telephony Requirements
10.2.2.3.2	Call Centre Telephony Requirements
10.2.2.3.3	Number Porting Requirements
10.3	**Additional Services Required**
10.3.1	Bulk Email Service
10.3.2	Bulk SMS Service
10.3.3	Cloud Management Services
10.3.3.1	Migration of Existing Servers and Services
10.3.3.2	SANParks E-Business Website Hosting, Support and Maintenance
10.4	**Security Services**
10.4.1	Security Operations Centre (SOC) Services
10.4.2	Vulnerability Assessment Services
10.4.3	Perimeter Protection Services
10.4.4	PCI DSS Governance and Monitoring Services
10.5	**Additional Services**
10.5.1	ICT Maturity and Innovation Services
10.5.2	Quality Assurance
10.5.3	IT Governance Scope of Work
10.5.4	Enterprise Architecture Services Scope of Work
10.6	**Additional Criteria to be Noted**
10.6.1	Geographical Capacity
10.6.2	Experience and Performance Measurement
10.6.3	Performance Criteria
10.6.4	Service Levels Required

10.1 **Core Services**

All services provided must comply with SANParks' internal policies, standard operating procedures, standards, and any other relevant governance requirements, which will be shared with the successful Bidder upon appointment. These internal requirements are consistent with recognised best practices.

Bidders are advised that service delivery will be governed by defined Service Level Agreements (SLAs), which form a critical component of this contract. SANParks requires the Bidder to adhere strictly to the timeframes, performance standards, and response commitments as set out in 10.6.4 Service Levels Required. These SLAs cover, but are not limited to, system availability, incident response and resolution times, change management processes, and reporting obligations. Compliance with these timeframes is mandatory, and SANParks reserves the right to impose penalties or apply contractual remedies should the Bidder fail to meet the agreed-upon standards.

10.1.1 Single Service Aggregator

SANParks is seeking to appoint a Single Service Aggregator (SSA) to take full responsibility for the management of services, contracts, and vendors within its ICT environment. The appointed SSA must demonstrate proven experience in coordinating and governing multiple service providers under a unified framework, ensuring accountability, efficiency, and compliance. Critical to this role is the capacity to provide robust contract governance across risk management, legal, auditing, and contract management functions, supported by appropriate technologies to effectively govern various contracts. In addition, SANParks requires the SSA to ensure the continuous presence of a Service Delivery Manager (SDM) on-site in Pretoria, with a suitably empowered delegate available to make decisions whenever the SDM is unavailable for more than two hours. This arrangement is essential to guarantee uninterrupted oversight, rapid issue resolution, and alignment with SANParks' operational and governance standards.

In your proposal, please describe your SSA methodology / Service Delivery Model, (SDM), to manage services following the SIAM approach for a Single Service Aggregator.

Please demonstrate IT Service Management in an ITIL-aligned service management structure with mature SIAM/ITSM processes and supporting tooling.

10.1.2 Centralised Single Point of Contact (SPOC) Service Desk Aggregator

The Bidder must be able to demonstrate that they can provide a service desk service to SANParks that will cater for all ICT-related incidents, problems, IMACDs, tasks, request fulfilment tasks and requests for information submitted by any user on any ICT application or related infrastructure supported by any service provider inclusive of SANParks internal support.

Note that SANParks have teams of support people for the applications listed below. The SPOC service must also include the management of these teams and incidents referred

to these teams. Therefore, licences on the service management software and access by these support teams to the software must be provided for —

- Tourism Property Management System – 4 people
- Loyalty Management System (CRM) – 3 people
- Business Process Management System – 4 people
- Financial and HR Systems – 2 people

The requirement is for a SPOC service.

SANParks users may not be referred to external or other SANParks internal support staff.

The agent taking the call must be able to determine the issue at hand, ask sufficient leading questions to determine the possible cause of the issue, attempt to resolve it as a first-line call, and refer the call to the appropriate identified support engineers for resolution.

The service desk remains the owner of the incident until resolved.

The service offering should include diligent following up of incidents through its lifecycle to final resolution.

Logged incidents may not be pended without express permission of either the user logging the call, their direct manager or the SANParks relationship manager.

Separate reporting for incidents relating to any major application in use by SANParks.

Please ensure the following points are taken into consideration in your proposal with regard to a service desk solution:

- licensing for up to 15 SANParks support staff to manage incidents assigned to them;
- the ability to give access for third party support agents, (approximately 15 users);
- the ability to manage these third party agents;
- the ability to handle incident management (average of 2500 – 3000 per month);
- the ability to address calls with severity 1 and 2 incidents;
- the ability to handle multiple incident logging channels such as via email, telephone, instant messaging platforms, and web forms;
- ability to clearly define and handle escalation processes;
- ability to handle support calls and requirements after normal working hours;
- the ability to provide comprehensive reporting per severity level, classification, location, application, user, and service;
- the ability to provide an integrated feed of all incidents, call statistics, IMACD and relevant metrics from Bidder's system into SANParks data warehouse on MS SQL

so that SANParks has access to the data for own use and analysis over and above what would be provided by the Bidder; and

- has the ability to provide comprehensive problem management, knowledge management, event management, request fulfilment and task management.

10.1.3 User Support

SANParks operates in a geographically dispersed environment across South Africa (refer to **Annexures 1K** and **Annexure 1L**). As tourism operations are essential to funding conservation activities, uninterrupted user functionality in these areas is critical. Any disruption affecting Tourism staff must receive priority attention within defined service levels.

Service Level metrics have been designed to reflect this priority. To meet these requirements, the appointed Aggregator must deploy permanent Field Service Engineers (FSEs) at core operational sites as follows:

Location	Minimum FSEs
Head Office (Pretoria)	4
Cape Town (Tokai)	3
Skukuza & surrounding towns (e.g. Hazyview, White River, Nelspruit, Malelane)	4 (minimum 2 in Skukuza)
Phalaborwa Gate / Town	2
Eastern Cape (Knysna / George / Port Elizabeth)	2

In addition, shared FSE's must be located within 2–3 hours' travel from remote parks to enable timely on-site support. Remote FSEs must be technically capable of assisting with both network-related issues and physical server support, including systems deployed at gates for security cameras and number plate recognition.

User support includes any ICT-related issue across authorised devices and operating systems, including desktops, laptops, tablets, mobile devices, connectivity, applications, cloud storage, printing, scanning, IP telephony, etc. Support must extend across Windows, iOS, Android and all approved devices and platforms.

Refer to **Annexure 1E** for completion.

The successful Bidder will be responsible for:

- User data backup, transfer, and restoration within 2 days upon request
- Building standard device images for use by the hardware vendor prior to delivery
- IMACD services
- Full maintenance and management of the CMDB for all hardware, software and configuration items, aligned to the SANParks Asset Register, including where applicable:

- User, Location, Functional Area (Tourism, Finance, HR, Conservation, ExCo, Board, Biodiversity Unit, Research, etc.)
- Asset Number / Serial Number
- Operating System and Office Version
- Local applications
- Make / Model
- Installation Date / Warranty Date / End-of-life

- Providing an integrated feed of all CMDB data into the SANParks MS SQL Data Warehouse
- Password management (process to be detailed in proposal)
- Software licence management
- Identifying training needs and assisting in processes to improve user awareness
- Monthly comprehensive reporting by Classification, Location, Application, User, and Service
- Recommending equipment upgrades and proactively managing hardware refresh cycles per site on a quarterly basis

10.1.4 User Device Configuration

Field Service Engineers (FSEs) are responsible for configuring user devices, including desktop computers, notebooks, printers and related peripherals. Due to the hardened security environment, users cannot install software or modify system configurations. This security framework includes encrypted internal hard drives and, where applicable, encryption of external storage devices.

When SANParks introduces new standardised computer models, senior FSEs must configure these devices according to SANParks' approved configuration standards. A master image must then be created and supplied to the designated procurement vendor(s) for preloading on devices before delivery to end-users. Final configuration and data transfer to the user occur at the site of deployment.

Support must also extend to senior users who utilise multiple devices (e.g. desktops, laptops, tablets and mobile phones). The service must therefore include management of Enterprise Mobility and Security (EMS) across multiple operating systems, including Windows, iOS and Android.

Minimum Requirements

- Configuration and setup of services across desktops, notebooks, tablets and mobile phones.
- IMACD services for desktop equipment completed within 3 business days.
- Preparation of new device images within 2 business days.
- IMACD support available at all SANParks sites.

10.1.5 Network Management (WAN, LAN and Internet)

The successful Bidder must manage and provision all SANParks network services—WAN, LAN and Internet—in accordance with approved SANParks standards and network build guides.

This includes the full Wide Area Network across multiple technologies (e.g. Diginet, Metro Ethernet, VSAT, Mobile Data), as well as management of Virtual Private Networks (VPNs) on routers and switches. Proactive monitoring of all network links and devices is required to ensure optimal performance, availability and early detection of faults. Where failures occur, the Aggregator must implement failover measures and replace faulty equipment promptly to maintain core IT operations. Labour and service costs for replacing faulty LAN equipment must be included in the bid; SANParks will provide the replacement hardware itself. Required network availability levels are defined in 11.6.5 - Service Levels Required.

Proposal Requirements

Your proposal must address the following—

- **IMACD Services:** Monthly comprehensive IMACD support for network-related changes
- **Preventative Maintenance:** Bi-annual preventative maintenance on all network equipment (switches, routers, wireless access points, cabinets, UPS units, etc.)
- **Network Monitoring & Management:** Proactive and reactive monitoring of all network components, including performance, configuration, outages, failures and improvements
- **Reporting:** Monthly reports covering network performance, utilisation, IMACDs, issues and problem trends
- **Network Segmentation:** Logical network segregation (VLANs) following security and best-practice standards
- **Network Documentation:** Monthly update and maintenance of all network diagrams, asset inventories and data flows in alignment with PCI DSS requirements
- **CMDB Maintenance:** Full maintenance of CMDB data for all network components
- **Third-Party Coordination:** Management and coordination of network-related services from external providers (e.g. Vodacom, MTN, Telkom, Cell C), including user access to cellular data, VPN and APN services
- **Availability Requirement:** Network uptime must exceed 99%, with no exclusions for third-party dependencies

10.1.6 Server Management

The detail of the servers and corresponding services in the environment are presented in **Annexures 1C** and **1D**.

Bidders should also note that although the environment is predominantly based on Microsoft, there are a few servers that run other operating systems such as Linux CentOS. The service offering should include the management of these servers and operating systems as described.

The management of any server, be it on premise or in the cloud, must remain the responsibility of the Aggregator that is appointed. The building or configuration of any server must follow the best practice standards as approved by SANParks, including sufficient hardening from a security requirement and logging of all administrator level user actions.

The services required must relate to the pro-active monitoring of all servers in SANParks, the associated maintenance, configuration, security standards, problem management, patching and upgrades thereof along with firmware upgrades, etc. as defined in ITIL® and following the guidance of relevant best practices.

A full set of Microsoft 365 Services will need to be managed and the Bidder is expected to have all relevant Microsoft Certifications. See **Annexure 1G Capability**. Bidders to note that the number of virtual machines indicated in the Annexures is indicative only, and is subject to change.

Please note the following requirements with regards Server Management—

- Server availability (>99%) 24x7x365 in High Availability mode
- Patch Management
  - within 24 hours for critical security patches
  - within 72 hours for high impact security patches
  - weekly for other important security patches
  - fortnightly for other patches
- Firmware is updated when required on a quarterly basis
- Annual Review to ensure Operating Systems are upgraded in consultation with application vendors – the Aggregator must drive the process
- Full Maintenance and Management of CMDB on all Hardware, Software and Configuration Items (CI)
- Management of any / all cloud infrastructure, software, platforms
- Quarterly Capacity planning is performed where applicable

- Full configuration / setup documentation of all servers and applications with emphasis on security standards
- Optimising server performance
- High Availability environment management
- High Availability testing every quarter
- Backup of servers, applications and data (Daily / Weekly / Monthly / Annually)

10.1.7 Database Administration

The database most commonly in use is Microsoft SQL. Please refer to **Annexure 1C** for details of the various versions of Microsoft SQL that are in use). Please note that some specialist applications make use of other databases such as MySQL in the LINUX environment.

The level of service required is that of experienced SQL database administrator service that must ensure that the database environment is configured per best practices, is secure and managed pro-actively. Databases must be maintained in current state in consultation with application owners. Services must encompass ITIL® fully.

When performance issues are experienced, the problem must be subject to focussed attention, speedy resolution and management processes must be followed to reinstate the database to a full working state with the least possible negative impact on business and users.

Continued advice on improving the environment must be provided and steps taken to optimise performance.

The following needs to be taken care of:

- Database availability >99% with 24x7x365 in high availability mode (where applicable)
- Quarterly review to ensure that databases are upgraded in consultation with application vendors. The appointed Bidder must drive this process
- Monthly full maintenance and management of CMDB on all databases
- Management of any / all cloud-based databases for IaaS and PaaS deployments
- Monthly capacity planning is performed where applicable
- Full configuration / setup documentation of all databases with emphasis on security standards after/when changes happen
- Database performance optimisation
- Disaster recovery testing every quarter

- Daily Backup of databases

10.1.8 Disaster Recovery Management

Business Continuity is paramount to the ICT services provided to the SANParks operations. Especially the tourism operations can't afford to have their services negatively impacted and processes must be put in place and tested regularly to ensure maximum uptime of these services and minimised risks to SANParks business.

SANParks requires a robust and fully documented Disaster Recovery (DR) strategy to ensure rapid restoration of critical systems and services in the event of a disruption. The appointed service provider will assume responsibility for the management of SANParks' cloud environment and will be tasked with designing, implementing, and maintaining a comprehensive recovery plan that aligns with industry best practices and regulatory requirements.

This plan must include clearly defined Recovery Time Objectives (RTOs) and Recovery Point Objectives (RPOs), regular testing of failover capabilities, and continuous monitoring of system health and data integrity. The successful Bidder will ensure that the DR strategy integrates seamlessly, enabling swift failover to alternate resources, minimising downtime, and safeguarding the continuity of SANParks' mission-critical operations.

SANParks requires the bidding party to provide this solution as a 'Disaster Recovery as a Service' solution such that billing only occurs when testing or utilising the service.

Please be aware that the following items need to be considered, over and above the details that follow in subsequent paragraphs:

- Ensuring all data is backed up according to the approved Backup SOP and standards on a daily basis
- Perform data restoration testing monthly
- Facilitate and perform Disaster Site data integrity testing quarterly
- Alerts on any critical events with immediate escalation
- Review of event logs on a weekly basis
- Immediate Alerts on configuration changes if not planned as part of Change Management process – Verify in any case against planned change and escalate if not commensurate with planned change
- Monthly Comprehensive reporting

Use the following points as guidelines for required functionality —

(Note – the Servers listed in Annexure 1D need to be protected, including any additional Servers/Services that may be added in the future).

10.1.8.1 *Backup and Recovery*

- Instant Recovery: Near-zero RTOs for VMs, databases, and files;
- Continuous Data Protection (CDP): Enables recovery to any point in time;
- Immutable Backups: Prevents encryption or deletion by ransomware;
- Granular recovery capabilities, including file-level, object-level, and application-consistent restores;
- Global search and predictive indexing of backup data for rapid identification and restore of files, VMs, or databases;
- Automated, policy-driven backup orchestration across on-premises and cloud workloads; and
- Data immutability and ransomware protection with write-once-read-many (WORM) storage options.

10.1.8.2 *Supported Workloads*

- Virtual: VMware vSphere, Microsoft Hyper-V, Other;
- Databases: Microsoft SQL Server, Oracle/MySQL, Other;
- Cloud: AWS, Azure, Google Cloud, Microsoft 365, VMware Cloud on AWS;
- SaaS: Microsoft 365 (Exchange, OneDrive, SharePoint, Teams), Other;
- Kubernetes: Centralized protection and management; and
- File Systems/NAS: Large-scale unstructured data backup and recovery.

10.1.8.3 *Storage and Archiving*

- Cloud Vault: Isolated, off-site archival of immutable data;
- Cloud Archival: Automated, scalable archival for compliance;
- NAS Cloud Direct: Efficient storage of massive unstructured datasets; and
- Integration with cloud providers for seamless tiering, archival, and geo-dispersed replication.

10.1.8.4 *Security and Compliance*

- Zero Trust Data Security™: Built-in architecture to prevent unauthorized access;
- End-to-end encryption in transit and at rest with integrated key management;
- Compliance support for GDPR, HIPAA, POPIA and other regulatory frameworks;
- Post-incident impact analysis and ransomware recovery insights; and
- Role-based access control and multi-tenancy support for secure operations and delegated administration.

10.1.8.5 *Automation and Integration*

- Policy-driven management: Automate backup frequency, retention, and SLA enforcement;
- Orchestration workflows to automate failover, failback, and application dependency mapping;
- Automated, non-disruptive DR testing with reporting for audit and compliance;
- API-first architecture for integration with ITSM, monitoring, and security platforms;

- ServiceNow and vRealize Automation: Lifecycle management and compliance automation; and
- Microsoft API integration for high-speed backup and restore in Microsoft 365 environments.

10.1.8.6 *Performance and Efficiency*

- Admin time reduction: Up to 90% less time spent on backup management;
- Lower TCO: Reduces data center footprint and operational costs by 30–50%;
- SLA-based monitoring and alerts to ensure RPO/RTO compliance;
- Scalability: Supports environments with tens of thousands of users and billions of files; and
- Built-in reporting and analytics for backup success, capacity usage, and compliance posture.

10.1.8.7 *Reporting and Alerting*

- Real-time monitoring dashboards showing backup, recovery, and replication status;
- Customisable alerting thresholds for RPO breaches, failed backups, job delays, or ransomware anomalies;
- Multi-channel notifications (email, SMS, SNMP, API integration into SIEM/SOC platforms);
- Automated compliance reporting with scheduled distribution for auditors and stakeholders;
- Trend analysis and forecasting to predict capacity requirements and performance bottlenecks;
- Incident reports with root cause analysis for failed or delayed jobs; and
- Centralised SLA compliance reports across workloads and sites.

10.1.8.8 *Deployment Models*

- On-Premises;
- Cloud-Native;
- Hybrid Cloud; and
- Backup-as-a-Service (BaaS) / Disaster-Recovery-as-a-Service (DRaaS) with pay-per-use billing for tests and failovers.

10.1.9 Mimecast Management

SANParks currently uses Mimecast as the email archive cloud service of choice with more than 10 years of email records archived in that environment. Included in the service is the basic spam and malicious content filtering service, branding, folder replication, stubbing, etc. In addition, Targeted Threat Protection (TTP) has also been introduced to deal with instances of Whaling and Spear phishing.

The successful Bidder is required to take over the current agreement from the vendor responsible for the relationship with Mimecast and manage it going forward, based on the vendor model of Mimecast.

SANParks currently has 2,500 users in the Mimecast service. This user count may change during the term of this award, and the Service Provider must be prepared to adjust services accordingly.

Please ensure the following is considered as part of your proposal:

- Ensure that the Mimecast email archiving and associated services including Targeted Threat Protection are managed.
- Perform required changes as per Change Management Process.
- Perform any requested data extract as reasonably requested from time to time.
- Manage Mimecast as Service Provider which includes taking over of any existing contractual agreement.
- Provide User Support for all Mimecast requirements where applicable.

10.1.10 Patch Management and Support

The appointed service provider shall implement and maintain a comprehensive Patch Management Service to ensure SANParks' ICT environment remains secure, resilient, and compliant. The solution must cover operating systems, third-party applications, and firmware across all endpoints, servers, and network devices. At a minimum, the patch management solution must provide —

- Centralised Patch Deployment: Ability to schedule, approve, and deploy patches across diverse environments (servers, endpoints, and network devices);
- Third-Party Application Support: Patch coverage for common productivity and security applications (e.g., browsers, Java, Adobe, etc.);
- Automated Patch Discovery: Continuous scanning to detect missing patches and vulnerabilities across the environment;
- Prioritisation and Risk Scoring: Intelligent prioritization of patches based on severity, CVSS scoring, and vendor advisories;
- Testing and Rollback Capabilities: Ability to test patches in controlled environments and roll back automatically if instability is detected;
- Compliance Enforcement: Policy-based enforcement ensuring endpoints and servers remain within defined patch compliance levels;
- Reporting and Audit Trails: Comprehensive reporting on patch status, compliance levels, and failed deployments with full audit logs;
- Integration: Compatibility with existing ITSM, monitoring, and security platforms for streamlined workflows;
- Scheduling and Bandwidth Control: Ability to schedule patch deployment by site/time window and manage bandwidth usage in remote or bandwidth-constrained locations; and
- Alerting: Automated alerts for failed patches, overdue updates, or compliance deviations.

10.2 **LAN/WAN**

10.2.1 Local Area Network Installation and Maintenance Services

This service is required for the installation of new network points, as well as the maintenance and repair of existing network points, at all SANParks sites. This service must also accommodate the expansion of the LAN to separate buildings via fibre optic or radio links at various sites.

Quotations may be required for additional services including, but not limited to, wireless access points and cabinets, provided these fall within the scope of this agreement. SANParks reserves the right to accept or decline any such quotation.

10.2.1.1 *Network Points*

This service should be costed into your proposal with the following three base costs —

- Fixed rate for the installation of a network point, regardless of the length of cable needed (up to a maximum of 100m of cable per network point);
- SANParks shall only reimburse ancillary costs, such as travel, in accordance with the applicable rates published by SARS; and
- Labour costs for installation of a network point, per hour (if not included in the fixed rate per network point as above).

This service should be costed into your proposal based on the anticipated volume of network points involved —

- Installation of 1,500 new network points over a 10-year period (an average of 150 new network points per annum), as and when required;
- New network points will be required for new sites which may not be accounted for in the above figures;
- Repair of 1,000 existing network points over a 10-year period (an average of 100 existing network points per annum), as and when required.;
- The price must include the complete installation including cabling, connectors, conduit, etc (excluding fibre/radio connections); and
- The price shall exclude the cost for LAN extensions to separate buildings/sites on the same premises via fibre/radio link.

10.2.1.2 *Expansion of the LAN*

This service should be costed into your proposal with the following base costs —

- Armoured fibre must be used for fibre connections due to environmental issues;
- Bidders must use multimode fibre (distances will be 1,000m max);
- Trenching may be required;
- All radio equipment used in the expansion of links must be ICASA approved; and
- Erection of poles may be required.

SANParks will provide accommodation in the relevant park as far as possible for quotation/installation needs. Where SANParks is unable to provide accommodation, the Bidder must include these costs in the quotation, in line with the National Treasury threshold for Government Institutions, as per the document published on National Treasury Website, **(NATIONAL TRAVEL GUIDELINE.pdf)** - https://www.treasury.gov.za/legislation/pfma/TreasuryInstruction/Annex%20A%20-%20NATIONAL%20TRAVEL%20GUIDELINE.pdf

10.2.2 Wide Area Network Services

SANParks requires the successful Bidder to design and implement a new Wide Area Network (WAN) as a priority project. SANParks has provided details of all site locations, existing connectivity infrastructure, and available towers that may be used at the Bidder's discretion (**Annexure 1F – WAN Pricing**). The appointed service provider must develop a complete WAN architecture and implementation plan that delivers high-performance, secure, and resilient connectivity to all SANParks sites. The solution must include built-in redundancy at every location to ensure uninterrupted operations and must be scalable to meet long-term requirements.

10.2.2.1 *Wide Area Network Requirements*

SANParks requires a managed WAN service from a single Value-Added Network Service Provider with access to wholesale data communication infrastructure from all major and any other network service providers.

The provisioning of last mile connectivity does not necessarily have to be by the same service provider, but the main Service Provider (Bidder) should manage any other Service Provider that provides last mile connectivity.

The WAN design and architecture must be reviewed and optimised for operational efficiencies.

SANParks experience with regards to VSAT has not been greatly successful due to high latency, contention and cost. SANParks would prefer VSAT be avoided wherever possible.

The proposed design must be included in the proposal.

All WAN equipment purchased will be owned by SANParks, and all designs shall belong to SANParks and must be shared with SANParks.

Over the anticipated ten-year duration of this contract, it is recognised that bandwidth requirements will continue to grow significantly, both in terms of volume and speed, driven by evolving technology, cloud adoption, and user demand. At the same time, market prices for bandwidth have historically fluctuated but generally trended downward due to advances in infrastructure and increased competition. To ensure the organisation benefits from these shifts, a structured review mechanism will be built into the agreement at 2 year intervals. This mechanism will allow for reassessment of

prevailing market rates and capacity requirements, ensuring that the contract remains cost-effective, competitive, and aligned to actual business needs over its full term.

The Bidding Party should cater for future growth in SANParks sites as well as the possibility of decommissioning sites that close.

10.2.2.2 *Internet Access Services*

SANParks requires a SD-WAN network with connectivity back to Teraco as well as local internet breakout for each site.

We require the following to be taken into account —

- Centralised Orchestration: All branches are managed from one central controller. Configuration, security, and traffic rules are pushed to branches without manual CLI work on each device;
- Dynamic Path Selection: Each branch can have multiple links (Fibre, LTE, satellite, broadband). SD-WAN monitors link health (latency, jitter, packet loss) and routes traffic dynamically across the “best available” link in real time;
- Direct Cloud Connectivity: Branches don’t need to hairpin traffic through the data centre. They can connect directly to the private cloud or public cloud services securely;
- Application Awareness: Traffic is steered based on application type (e.g., tourism reservation system, VoIP, video conferencing) to prioritise critical workloads and avoid congestion;
- Security Integration: SD-WAN can embed next-gen firewall, segmentation, and even tie into SASE (Secure Access Service Edge), ensuring branches securely connect to the private cloud; and
- Resilience: If one link fails (e.g., fibre cut at a park), traffic automatically shifts to an alternate path (LTE, satellite) with minimal disruption.

Management of Internet Access should also be read together with security services as described under paragraph 4.

Please see **Annexure 1F – WAN Pricing**, showing the locations as well as current and future bandwidth requirements.

10.2.2.3 *IP Telephony Services*

10.2.2.3.1 General Business Telephony Requirements

SANParks requires the provision and ongoing support of a comprehensive telephony solution to be used. While Microsoft Teams Calling is the preferred platform, (as SANParks currently subscribe to Microsoft 365 E5 Licenses), SANParks is open to alternative solutions that exceed the functional and performance requirements of Microsoft Teams Calling. The solution must incorporate the following services: Telephone Cost Management System, Contact Centre Management, Contact Centre Email Management System, Contact Centre Voice Recording System, Unified Communications, user instruments/devices, and

Least Cost Routing. The solution must also provide for video conferencing and teleconferencing. The successful Bidder will be responsible for designing, implementing, and maintaining a secure, scalable, and cost-efficient telephony architecture that integrates seamlessly with SANParks' network and operational requirements.

The following items must also be addressed as part of the Bidder's responsibilities:

- Provision of a unified telephony platform supporting both on-premise handsets and softphones (desktop and mobile clients).
- Support for fixed line, mobile extension, and softphone endpoints under a single number (single number reach).
- Voicemail services with voicemail-to-email functionality.
- Caller ID, call forwarding, call hold, call park, and call transfer functionality.
- Provide user support on IP telephony issues
- Hunt groups and ring groups for departmental lines (e.g., Finance, HR, Tourism).
- Setup of new IP phones or swapping out where required from existing SANParks stock
- Auto-attendant for main business lines, with configurable hours and routing.
- Support for extension dialling, including short codes and internal directory integration.
- Multi-device ringing capability (desk phone, PC, mobile simultaneously).
- Your solution must support High-definition voice quality with QoS support across the SANParks network.
- Least Cost Routing (LCR) and call breakout for local, national, and international calls.
- Call detail records (CDR) and billing analysis by department / cost centre.
- Ability to record selected non-call centre calls for compliance (e.g., Finance, HR).
- Integration with SANParks Active Directory for authentication and user provisioning/de-provisioning.
- Integration with CRM and email systems for click-to-dial and screen pop-up.
- Conference calling and audio bridging capability.
- Support for hot desking and extension mobility (users log into any handset).
- Failover and business continuity features (redundant SBCs, cloud failover, PSTN breakout).
- SLA for Monthly reporting on call volumes, call quality, outages, and SLA adherence and resolution (e.g., priority 1 faults resolved within 4 hours).

10.2.2.3.2 Call Centre Telephony Requirements

The Telephony Solution also needs to include a solution for the Call Centre, (separate from the Above solution) which meets the following requirements —

<u>Inbound Call Handling</u>

- Skill-based routing, IVR selection, or customer history;

- Automatic Call Distribution (ACD) to available agents;
- Call transfer between agents or queues;
- Multi-queue capability (agents can join/leave multiple queues);
- Call overflow and interflow handling;
- Call queuing with estimated wait time announcements and queue position notifications; and
- Call back functionality for customers during peak volumes.

Agent Interface

- Web-based or desktop application;
- Unified dashboard with active and queued interactions;
- Access to customer information and interaction history;
- Integrated knowledge base and internal support tools;
- Real-time presence and status management (Available, Break, Offline, etc.);
- Auxiliary work codes (tea break, lunch, training) with reporting on usage frequency;
- Wrap-up time and control of interval between calls;
- Conference call capability; and
- Internal messaging for real-time collaboration during calls.

Supervisor Tools and Access Controls

- Silent monitoring (whispering, barging, coaching);
- Live monitoring of calls and agent performance;
- Real-time dashboards and wallboards;
- Remote ability to log agents in/out for workforce management;
- Performance KPIs (AHT, FCR, service level adherence, abandonment rate, etc.);
- Quality management and evaluation tools;
- Workforce management integration (scheduling, forecasting, adherence);
- Comprehensive logging of all Supervisor actions (e.g., call monitoring, barging, recording access, agent adjustments, queue management changes);
- Tamper-proof, immutable audit logs;
- Time-stamped entries for every action;
- Secure storage and accessibility of logs for audit and compliance review; and
- Retention of audit logs for a minimum of 5 years, or longer if required by applicable legislation or regulatory frameworks.

IVR (Interactive Voice Response)

- Customisable IVR menus and workflows;
- Ability to record ad-hoc IVR messages; and
- Customer identification by unique identifier (e.g., client code, Wild Card number) via Microsoft Dynamics 365 integration.

Reporting and Analytics

- Real-time and historical reporting;

- Standard reports: call volumes, answered vs received, abandonment rate, average handle time (AHT), service level adherence, occupancy %, idling time, shift time, ringing time, requeued/missed calls, overflow/interflow calls, ACD vs non-ACD calls, short handle calls;
- Custom report builder with export to PDF, Excel, CSV;
- Automated and scheduled report distribution; and
- First login/last login timestamps for agents.

Call Recording and Quality Monitoring

- Full, on-demand, or random recording options;
- Storage and playback with tagging and commenting;
- Supervisor evaluation templates and scoring;
- Redaction tools for PCI/PII compliance;
- Retention controls to ensure recordings comply with legal and regulatory requirements; and
- Retention of call recordings for a minimum of 90 days, or longer as mandated by applicable legislation, contractual obligations, or regulatory compliance requirements.

Integration Capabilities

- API access for integration with CRM, ERP, loyalty, and other systems and
- Native integration with Microsoft Dynamics 365 for customer data and identifier recognition.

Omnichannel Integration (Future-Proofing Recommendation)

The proposed solution should be designed and specified to allow for future integration with multiple communication channels. At a minimum, the system architecture should support —

- Email Integration – enable two-way interaction with customers via email, with automatic case creation, tracking and response management;
- SMS Integration – provide outbound and inbound SMS capability, with delivery status tracking and message threading;
- WhatsApp Integration – support direct integration with WhatsApp Business API for two-way text, image, and file sharing, ensuring messages are logged within the call centre system; and
- Additional Channels – allow extension to other digital and social channels (e.g., webchat, Facebook Messenger, mobile app push notifications), through standard APIs or pre-built connectors.

System Capacity and Scalability

- Support for high call volumes with no artificial queue limits;
- Dynamic queue management to prevent engaged tones; and
- Scalable architecture to handle peak demand without service degradation.

10.2.2.3.3 Number Porting Requirements

The successful Bidder will be responsible for porting all numbers owned by SANParks from the current provider to the relevant systems.

10.3 **Additional Services Required**

10.3.1 Bulk Email Service

SANParks requires a bulk email service that will enable the running of email marketing campaigns and communication with clients.

The service should include assessing the content and volume of each campaign to ensure that SANParks' domain is not blacklisted.

In addition, any such campaign must allow for an unsubscribe facility for different types of email campaigns, e.g., loyalty, marketing, general information, emergency communication, etc.

When unsubscribing, the database must be updated and allow for updating of other SANParks CRM type systems through web services exposed and consumed on BizTalk/Azure integration services.

Please allow for approximately 12 campaigns per annum and a total of 700 000 emails per annum, which will increase by 100 000 emails per annum on average.

Provide a description of the proposed solution.

Indicate what steps will be taken to prevent black-listing of SANParks domain.

Describe the proposed unsubscribe function that will be provided.

10.3.2 Bulk SMS Service

SANParks requires a bulk and ad-hoc SMS service that will enable the running of SMS marketing campaigns and communication with clients, as well as sending of alerts based on events from within the SANParks applications and environment.

In addition, any such campaign must allow for an unsubscribe (opt-out) facility for different types of SMS services campaigns, e.g., loyalty, marketing, general information, emergency communication, alerts, etc.

When opting out, the database must be updated and allow for updating of other SANParks CRM type systems through web services exposed and consumed on Azure integration services.

Please allow for approximately an average of 800 000 SMS messages per month.

Provide a description of the proposed solution.

Describe how the usage of SMS will be managed and billed to SANParks.

Describe the proposed opt-out function that will be provided.

Explain how the opt-out responses will be integrated through web services exposed and consumed on Azure integration services.

10.3.3 Cloud Management Services

SANParks currently operates within a managed cloud environment that supports its critical business applications, data storage, and operational workflows.

10.3.3.1 *Migration of Existing Servers and Services*

It is preferable, though not compulsory, to utilise Teraco as the designated data centre, given that SANParks already has existing infrastructure hosted within Teraco facilities. SANParks is currently running its own infrastructure from Teraco, together with its IaaS environment, and the present Internet breakout is also terminated at Teraco, which makes business integration significantly easier. Leveraging Teraco therefore ensures continuity, operational efficiency, and seamless integration with current systems, while also providing established connectivity with leading service providers. However, to maintain flexibility and avoid limiting competition, Bidders may propose alternative data centre solutions, provided they meet or exceed the required security, compliance, and performance standards.

Please note that the current SANParks owned infrastructure is composed of both production and development machines, all running on Physical hardware as indicated in **Annexure 1C**. Most of the production component of this infrastructure is part of a project that is being decommissioned and it is anticipated that this will occur within the next 12 months or sooner. (See RoomSeeker on **Annexure 1C – SANParks Owned Equipment**).

The appointed service provider will be required to —

10.3.3.1.1 Assume full management responsibility for the existing SANParks infrastructure located at Teraco Data centre. (Refer **Annexure 1C – SANParks Owned Equipment**);

10.3.3.1.2 The bidding party must migrate the existing Private cloud workloads, (located at Teraco), (refer to **Annexure 1D – Private Cloud Pricing**), to a new private cloud, which must be located at Teraco;

10.3.3.1.3 The development component of the SANParks owned equipment needs to be migrated to a low-cost solution whereby billing occurs on a ‘Pay as you use’ basis;

10.3.3.1.4 The balance of the production machines will then need to be migrated to the new private cloud, see point 2 above. The production machines that become redundant due to the completion of the above-mentioned project can then be decommissioned; and

10.3.3.1.5 A key deliverable will be the design and implementation of a high-availability architecture to enhance system resilience, reduce downtime risk, and ensure continuity of critical services across all SANParks operations. The intention is to grow the maturity in the cloud from the current Cloud Maturity Model (CMM) level 1 (CMM 1 – Ad hoc) to CMM level 5 (optimised and pro-active) —

- The cloud environment must comply to the PCI DSS;
- The cloud environment must comply to all relevant ISO and Security standards;
- The cloud service must cater for full redundancy and / or high availability configurations in support of an always-on model of service; and
- The immediate cloud requirements that must be catered for as is described under 10.3.3.

Note - as virtual machines may be provisioned or decommissioned in line with operational requirements, Bidders must ensure their solutions and costing models accommodate this level of flexibility. SANParks will carry the cost of actual usage; therefore, proposals must reflect a scalable, adaptable environment that allows for seamless adjustment of resources without service disruption or unnecessary fixed costs.

10.3.3.2 *SANParks E-Business Website Hosting, Support and Maintenance*

The public, customer-facing, SANParks website (www.sanparks.org) presents an accessible portal for all e-commerce, promotional, services and general information sharing. The SANParks E-Business and Web division manages and facilitates all online, web-enabled applications to facilitate e-commerce and systems integrations solutions such as, reservations, online Card Not Present payments, Fundraising, Gate tickets, Wild Card and Donations. The SANParks website also supports and hosts access to the SANParks Forums, the Webcams and the core SANParks business divisions and units such as: Travel, Conservation, Social-Economic Transformation and Corporate sections of the website.

<u>On a core, foundational level, the following must be considered and included</u> —

The website hosting is based on Open Source Hosting and Services principles —

- Web Servers - Apache or Nginx;
- Databases - MySQL or Postgres;
- Scripting language – PHP; and
- Hosts – Linux.

SANParks E-Business servers are running and hosted in the Azure tenant.

SANParks website servers and hosting must adhere to strict PCI DSS audits and compliance and must be contained and managed by strict and appropriate firewall, routing and WAF implementations.

SANParks Servers must have an uptime of at least 99.9% (3 Nines).

All Servers in the E-Business web support must have a backup system and methodology in place for one full rotation backup and restore.

Development, Staging and Prototype web servers must be restricted and protected by relevant VPN or Zero Access systems.

Backup procedures and measures must include Development, Staging and Prototype servers.

Assistance with the implementation of new Payment merchants integrated with SANParks web payments gateways (in line with PCI requirements).

Management and facilitation of audits and compliance with PCI requirements by engaging with relevant and applicable PCI DSS compliance companies.

On a Support and Maintenance level, the following activities are required (but not limited to) —

Assisting with facilitating and setting up of new web hosts (including database (MySQL, MariaDB, Postgres or others), frameworks or languages (PHP, Laravel, Angular, Node, Composer etc.) and Web Server systems (Apache and/or Nginx)).

Assisting with and ensuring advanced and proper routing, aliasing, htaccess, rewrite rules and module loading.

Ensuring that all integrations, external and/or internal, are working properly and that security and rigidity of services and communications are ensured.

Ensure that all applications and services on all servers in the E-Business web domain are patched and updated in accordance with AG Audits, IT Security and PCI compliance requirements.

Ensure that logs of all patches and updates are kept and that all patching and updates are managed and governed in accordance with the Change Management and Change Control requirements.

Design, run and manage Monitoring, early detection and early failure avoidance systems such as Site uptime checking (Pingdom, Uptime Kuma) with at least 3 points of notification (SMS, Email and Push Notification Services).

General and ad hoc support to SANParks management, webmaster, reservations, E-Business and SANParks general IT support services staff in accordance with SLA targets and support tiers.

Ensuring the maintenance of all servers to ensure high availability and stability - includes monitoring capacity, traffic, load and performance impacts.

Support must include setting up and assisting IT/ITC, IT Security and the SANParks IT Support partner with DR testing as this relates to the SANParks E-Business web component.

On a code and application level, support includes—

Ad-hoc and additional development of new systems, enhanced systems, mobile application (linked to SANParks web), APIs (Server and/or Client).

Development or assisting with components of development for Restful APIs or SOAP services.

Integrations with (but not limited to): CallPay (or other payment gateways), RoomSeeker (or other Reservations systems), BizTalk and CRM (or any other relevant internal CRM and ERP system).

Manage and contribute to proper code and system version controls and DevOps (Azure DevOps as is standard in SANParks).

Working with and assisting SANParks E-Business Webmaster, Web Systems Analyst, Developers (Internal) and Senior Manager E-Business.

Provide Project Management, Project Planning and Project documents and capturing using tools such as: Jira, Slack, Teams and Azure DevOps with complete and auditable logs and documents for projects.

Assist with and setting up of UAT/SIT and Change Management of all Web related projects.

The skills and expertise relevant and preferable for the support of SANParks Web Site —

- Expert knowledge of Linux Operating Systems (CentOS);
- At least 5 years in system admin and technical support on Linux systems with high level proficiency in scripting, bash, setting up and maintaining a LAMP, LNMP, LNPP stack (Linux, Apache, MySQL and PHP / Linux, Nginx, Postgres and PHP / Linux, Nginx, Postgres and PHP); and
- Expert knowledge of internal and external, system to system, API level integrations and integrations security.

Experience with and knowledge of —

- Change Management and Governance requirements and principles;
- Working with third party providers, Outsourced support service providers and internal SANParks Stakeholders and Clients; and
- Consultation and collaboration with SANParks internal development teams, system admins and stakeholders on existing and new projects.

10.4 **Security Services**

IT Security is very important to SANParks, and as such, SANParks seeks a managed security service provider capable of delivering comprehensive, scalable, and resilient cybersecurity solutions aligned with its operational and compliance requirements.

The selected Managed Security Services Provider (MSSP) will be responsible for delivering a comprehensive suite of cybersecurity services that protect SANParks' digital assets, infrastructure, and sensitive data across its national footprint. The scope includes —

- Security Operations Center (SOC);
- Endpoint and Perimeter Protection;
- Identity and Access Management;
- Vulnerability Management;
- Email and Network Security;
- Threat Intelligence and Reporting;
- Compliance and Governance;
- Incident Management; and
- Certificate Management.

The implementation of managed IT security services must achieve the following —

- Strengthen SANParks' cybersecurity resilience;
- Ensure compliance with national and international standards (e.g., POPIA, GDPR, ISO 27001, PCI DSS);
- Support digital transformation and secure cloud adoption;
- Provide real-time visibility and reporting across all threat vectors; and
- Enable proactive risk management and continuous improvement.

SANParks also transacts using electronic payment facilities and hence must comply with the Payment Card Industry Data Security Standard (PCI DSS) which is specified as a separate required service under paragraph 10.4.4.

Security Incidents are a cause for potential concern and, as such, should be treated with circumspection and managed carefully. This includes understanding the nature of the incident, its possible and actual impact, the root cause, the resolution taken to restore services, and the steps taken to prevent future similar incidents. For this purpose, SANParks has included security incidents as a focus area in its Incident Management Procedure.

The management of Security Incidents is part of the required services in this Bid.

Over and above these requirements, the following specific security services are sought.

10.4.1 <u>Security Operations Centre (SOC) Services</u>

SANParks requires the following services from a SOC —

Security Information and Event Management (SIEM)

- Logs of actions taken by users with Administrator-level access on Infrastructure must be enabled —
  - Servers;
  - Operating Systems;
  - Databases;
  - SANParks website;

- Domain;
- Routers;
- Switches;
- Wireless Access Points; and
- Applications – User access management and administrator access.

- Centralised Log Management (CLM) is required;
- Measures must be in place to prevent log file tampering. Administrators may not be able to turn logging off or change the log files or rules without proper authorisation;
- The SOC service provider must analyse the log files and highlight any events that appear to be abnormal and that may compromise security in SANParks;
- These events / incidents must be reported to the appropriate governance structure in SANParks;
- These events/incidents must be investigated, and the outcome reported to SANParks; and
- Corrective measures to prevent serious compromising events must be implemented following normal change management processes.

Security monitoring and reporting service on all Internet facing applications

- Website;
- Staging / development server for Website;
- Trickle feed of room availability from Tourism database to online reservations;
- Web services between online reservations and tourism application; and
- Loyalty system client data management application.

Additional monitoring services should include the following —

- Intrusion Prevention;
- Intrusion Detection; and
- Data loss Prevention.

The successful Bidder must ensure this service is provided either through their own capabilities or by overseeing and managing a partner that offers these services under the direct management of the successful Bidder.

10.4.2 Vulnerability Assessment Services

The service provider must —

- Perform ongoing Scans;
- Conduct internal and external vulnerability scans on all in-scope systems on an ongoing basis;
- Ensure both authenticated and unauthenticated scans are performed to provide comprehensive coverage;
- Use Recognised Tools;
- Utilise an industry-recognised vulnerability scanning solution that is widely accepted in the market (for example, tools aligned with PCI DSS Approved Scanning Vendors);
- Tools must be able to cover operating systems, databases, applications, network devices, and cloud environments;

- Maintain Compliance;
- Ensure scans comply with relevant regulatory and industry standards such as PCI DSS, ISO 27001, or other applicable frameworks; and
- Provide evidence of compliance where required.

Reporting and Remediation Support —

- Deliver reports weekly, including increases and decreases of total vulnerabilities;
- Deliver detailed reports highlighting vulnerabilities, severity ratings such as CVSS, and remediation recommendations;
- Provide prioritisation guidance to address high and critical vulnerabilities; and
- Support SANParks in verifying that remediation actions have been effective through re-scans.

Management and Oversight —

- Manage the licensing, updates, and configuration of the scanning solution;
- Ensure scanning signatures and detection capabilities are kept up to date to identify emerging vulnerabilities;
- Provide dashboards and metrics on vulnerability trends over time;
- Integration with Security Operations;
- Coordinate with SANParks SOC for vulnerability event correlation and risk reporting; and
- Escalate critical findings immediately to SANParks security governance structures.

The annual licensing cost of the tool must be managed by the successful Bidder.

This service does not include penetration testing. Penetration testing will be conducted by independent service providers on a bi-annual basis to provide assurance that the SANParks environment is not compromised.

10.4.3 Perimeter Protection Services

SANParks' network architecture is composed of three logically distinct zones —

- Wide Area Network (WAN) with local internet breakouts at various operational locations;
- Public Cloud Environment (hosted in Microsoft Azure), where web-facing assets like the SANParks website and reservation services reside; and
- Private Cloud Environment, where back-office systems, enterprise workloads, and internal applications are hosted.

The SANParks network supports over 2,500 employees, multiple field locations, and high-volume public-facing transactions. The environment is subject to seasonal spikes in tourism-related traffic, making resilience and scalability essential. Cyber threats pose direct risks to conservation funding, reputational trust, and compliance with South African data protection law (POPIA).

One of the objectives of this tender is to implement a comprehensive, managed perimeter protection solution that spans all three zones and aligns with a Secure Access Service Edge (SASE) framework. The solution must, at a minimum, improve SANParks' security posture, enhance secure remote access, and protect both internal and public-facing systems.

The solution must, at a minimum, not only block malicious traffic but also deliver continuous threat intelligence updates, forensic visibility into attack vectors, and measurable improvement in security maturity over the contract term. Bidders must, at a minimum, demonstrate how their service integrates with SANParks' incident response procedures and SOC operations.

The solution should deliver —

- Zero Trust Network Access (ZTNA) for all users, both on-site and remote;
- Comprehensive Web Application Protection including —
  - Web Application Firewall (WAF);
  - DDoS protection;
  - Bot mitigation; and
  - Content Delivery Network (CDN) capabilities.
- DNS Security to monitor and manage DNS queries, block malicious domains, and enhance visibility;
- Application Acceleration and Resilience, ensuring performance and scalability;
- Threat intelligence integration, including real-time updates from global feeds and local contextualised alerts;
- Centralised visibility dashboard with role-based access for SANParks security teams; and
- Full audit logs, retained for a minimum of 12 months, with export options for compliance and forensic investigations.

Managed Perimeter Protection Services must, at a minimum, include —

- Firewall and Perimeter Enforcement;
- Fully managed firewalls at all SANParks entry points (on-site and cloud);
- Centralised configuration and consistent policy enforcement across environments;
- Proxy capability for secure outbound user traffic filtering;
- Next-Generation Firewall (NGFW) features including application awareness, SSL/TLS inspection, and sandboxing;
- High availability (HA) configuration with defined failover times;
- Cloud-Based Website and Application Protection; and
- Protect the SANParks public website and related applications (hosted in Azure).

The solution must, at a minimum, support —

- Single-location website —
  - HTTP and HTTPS traffic only;
  - No VLAN segmentation; and
  - Fair usage: 30GB/day bandwidth, 100 concurrent connections/day.

Cloud-based WAF must, at a minimum, provide: OWASP Top 10 threat protection

- SSL offload and verification;
- SQL Injection, XSS, and Remote File Inclusion protection;
- DDoS detection and mitigation;
- Bot scraping protection;
- Payment gateway traffic validation and sanitization;
- Malware detection, backdoor/shell identification;
- Website health and SSL certificate checks;
- Continuous monitoring with real-time alerting;
- Weekly security reporting and forensic support;
- Site uptime guarantee of 99%;
- PCI-DSS compliance features (integrity monitoring, secure log storage);
- Full API protection and visibility (for future mobile app integration); and
- Geofencing and IP reputation-based blocking.

Site Accelerator and CDN Features

- Low-latency delivery (<100 ms);
- Load balancing and high availability for web services;
- Traffic analytics and visitor insights;
- Dynamic content caching to handle seasonal spikes in demand; and
- Disaster recovery options for web assets hosted outside primary cloud region.

Additional Security Capabilities

- Intrusion Detection System (IDS);
- Intrusion Prevention System (IPS);
- Data Loss Prevention (DLP);
- Email and telephone-based security support —
  - Unlimited incident support and forensic response
  - Proactive outreach on high-risk alerts
- Endpoint integration capability for consistent policy enforcement; and
- AI-driven anomaly detection to identify insider threats or unusual activity.

Service Management and Customisation

- Custom rule support for WAF (1–3 hours/month);
- Daily review of high-risk alerts;
- New plugin/security change reviews; and
- All services must, at a minimum, be delivered as fully managed by the provider.

Minimum service levels must be clearly defined, including —

- Incident response SLA (e.g., critical alerts triaged within 15 minutes);
- Change request SLA (e.g., implemented within 48 hours); and
- Reporting SLA (weekly operational, monthly executive).

Providers must assign a dedicated account manager and conduct quarterly strategic reviews.

Bidders must also provide a three-year service roadmap (e.g., AI integration, quantum-resilient encryption).

10.4.4 PCI DSS Governance and Monitoring Services

The Bidder must describe how they will render these services, focussing on the skills that they will bring to the table and previous experience in this regard.

Annual PCI-DSS Recertification of SANParks —

- The Service Provider shall be responsible for ensuring that SANParks undergoes annual PCI-DSS recertification at the level required for its operations;
- The Service Provider must either —
  - hold the relevant accreditation to perform PCI-DSS assessments directly; or
  - formally appoint and manage an accredited Qualified Security Assessor (QSA) to perform the assessment on behalf of SANParks.

Scope of Certification

- The Service Provider must ensure that the annual assessment covers all cardholder data environments (CDEs), systems, processes, and networks within SANParks that fall under PCI-DSS requirements; and
- Any changes in SANParks' environment (new applications, infrastructure, or services) must be incorporated into the scope of the annual review.

Deliverables

The Service Provider shall provide SANParks with the following, within 30 days of recertification completion —

- Valid Report on Compliance (ROC);
- Valid Attestation of Compliance (AOC); and
- Executive summary report outlining findings, gaps, and remediation steps (if any).

Remediation Management

- Where non-conformities are identified, the Service Provider shall assist SANParks in developing and implementing a remediation plan; and
- The Service Provider is responsible for tracking remediation to closure and ensuring any follow-up validation required for PCIDSS compliance is completed.

Ongoing Compliance Support

- The Service Provider must provide SANParks with guidance, monitoring, and advisory services throughout the year to ensure continuous PCIDSS compliance, not only during the audit window; and

- This includes support for policy updates, system changes, vulnerability remediation, and evidence gathering.

SANParks estimates approximately 200 hours per annum for advisory services; these should be costed in the proposal. Unused hours may not be billed and can be carried over to the subsequent period.

The independent QSA requirement must be based on 40 hours per annum.

10.5 **Additional Services**

This model is based on a single Service Aggregator for all ICT services for SANParks. Bidders are invited to propose additional services that align with SANParks' operational needs and provide value-add.

The Bidder is required to include these services in their response and provide the following —

- The framework that will be followed to provide these additional services;
- A detailed cost breakdown for the proposed additional services, including hours where applicable, as proposed in this bid;
- Noting that SANParks may not use these services every month, quarter or year and will only be billed for hours spent on the assignment; and
- Any unused hours from any period may be rolled over to a next period.

10.5.1 <u>ICT Maturity and Innovation Services</u>

The information and communication technology environment is constantly changing with new innovative ideas and technologies becoming available nearly daily. SANParks prefers not to be on the bleeding edge of new technologies, but most definitely seeks to capitalise on proven technologies to improve the product offerings and supporting ICT environment. Together with improvement in Governance, SANParks continuously seeks to improve overall service delivery maturity. This is particularly challenging given the distributed environment within which SANParks operates where users are in remote rural areas where first world communication challenges exist. Added to this are the prescripts relating to the natural environment and place of sense that may require Environmental Impact Assessments and / or Environmental Management Plans when infrastructure is required to be added to areas under management in accordance to the National Environmental Management: Protected Areas Act 57 of 2003.

It is envisaged that the successful Bidder should drive an innovation and maturity agenda together with SANParks. This would require meeting with the management of SANParks at least quarterly where relevant topics and innovative ideas can be discussed and from where specific initiatives can be identified to be put forward for SANParks to consider and if agreed to, to oversee the value-add successes of these initiatives.

This would require that the successful Bidder should expand on their knowledge of SANParks, its business, challenges and identify opportunities.

Quotations will be requested for ad-hoc IT services / projects within the scope of work of this tender.

Bidders are to provide an overview of the experience they will be bringing to the table regarding similar assignments, skills, qualifications and capability.

The winning Bidder will be expected to attend an annual workshop with SANParks to review the growth or scaling back of the infrastructure and to help facilitate budgeting requirements for the year ahead. The winning Bidder will continually keep SANParks updated with regards to asset management of the infrastructure.

10.5.2 Quality Assurance

SANParks requires the successful Bidder to assist our Internal Auditors with access to whatever systems, tools metrics etc as required by them to complete their functions.

10.5.3 IT Governance Scope of Work

SANParks requires the ad-hoc services of a Governance Risk and Compliance, (GRC), professional to assist in the following —

- Provide advice on governance related issues i.e digital strategy implementation, audit reports and ICT operational planning;
- Review current governance model, polices, procedures and operations;
- Select suitable and agile frameworks and standards in line with our strategies and business model;
- Propose and advise on governance model and organisational structure;
- Draft set of policies and procedures for efficient and optimum processes and operations;
- Provide a brief implementation roadmap including induction sessions for senior management and ICT team;
- Assist in preparation of quarterly and annual reports; and
- Prepare advice on policy issues including research, drafting tasks, think-pieces, policy papers, consultation, data analysis, decision-making papers, etc.

10.5.4 Enterprise Architecture Services Scope of Work

Link the mission, strategy, and processes of the organization to the IT strategy and document this using various architectural models or views that show how the current and future needs of the organization will be met in an efficient, sustainable, agile and adaptable manner.

Develop a comprehensive understanding of the current processes related to application design, architecture, software development, IT infrastructure, hosting and maintenance, database management, IT security, controls, document management, system performance and other applied business operations, practices and procedures of the organization applications.

Evaluate the efficiency and sustainability of the current business and IT processes, procedures, controls, and methodologies.

Identify gaps, risks, issues and opportunities to meet SANParks' needs.

Develop recommendations to ensure scalability and sustainability of the IT environment applications, eliminate or reduce software and process inefficiencies, increase productivity, and create new functionalities that benefit the cap-and-trade program.

10.6 **Additional Criteria to be Noted**

10.6.1 Geographical Capacity

Bidders are required to address in detail how they will service the geographical locations of SANParks different locations. Refer to 1 for a listing of the SANParks sites as well as maps indicating their different locations.

Proposals should indicate clearly amongst others the capacity and capability they currently have geographically regarding —

- Human resources and staff complement;
- Location of dedicated staff or offices or sub-contractors from where the sites will be serviced, considering the proposed Service Level requirements; and
- Where capacity at a site doesn't exist, the Bidder is required to indicate what their plans are to create the capacity to serve SANParks.

10.6.2 Experience and Performance Measurement

Bidders should illustrate their experience relevant to the provisioning of the services described in this bid. This should be done by documenting the following —

- The Bidder must list contactable reference sites that they are currently providing services that are similar to SANParks requirements. Refer to **Annexure 1H – References**; and
- The listing should include a description for the services that are provided to these reference sites.

10.6.3 Performance Criteria

SANPARKS RESERVES THE RIGHT TO APPLY FINANCIAL PENALTIES WHERE THE SUCCESSFUL BIDDER FAILS TO MEET THE MINIMUM SERVICE LEVELS DEFINED IN THE SERVICE LEVEL AGREEMENTS (SLA'S). THESE PENALTIES WILL SERVE AS A MECHANISM TO ENSURE ACCOUNTABILITY AND SERVICE EXCELLENCE. THE SPECIFIC PENALTY STRUCTURE, INCLUDING THRESHOLDS, FINANCIAL DEDUCTIONS, AND ESCALATION PROCEDURES, WILL BE FINALISED AND AGREED UPON DURING SLA NEGOTIATIONS WITH THE APPOINTED BIDDER. BIDDERS ARE THEREFORE ADVISED TO TAKE INTO ACCOUNT THE NEED FOR CONSISTENT PERFORMANCE AGAINST THE AGREED TIMEFRAMES AND QUALITY STANDARDS WHEN PREPARING THEIR PROPOSALS.

10.6.4 Service Levels Required

24-hour operations	< 2 hours
(Includes all web-based transactions and associated servers, applications and networks)	
Severity 1 – Immediate response, Targeted resolution within 2 hours	
7 day per week Tourism operations – Times to correspond with SANParks published gate times per Park / camp (See https://www.krugerpark.co.za/Kruger_Park_Travel_Advisory-travel/kruger-park-gate-times.html) plus all scheduled overnight services / processes	< 4 hours
(Relates to central systems for Tourism business as well major site failures where more than 50% of business capability, including printing is lost)	
Severity 2 – Immediate response, Targeted resolution within 4 business hours	
7 day per week other operations – 07:30 to 17:00	< 4 hours
(Relates to all central systems as well major site failures where more than 50% of business capability, including printing is lost)	
Severity 3 – Immediate response, Targeted resolution within 4 business hours	
7 day per week Tourism User support – 06:00 to 19:00	< 6 hours
(Relates to users in Tourism roles issues negatively impacting on business	
Severity 4 – Immediate response, Targeted resolution within 6 business hours	
7 day per week other User support – 07:30 to 17:00	< 8 hours
(Relates to all other users' roles with issues negatively impacting on business)	
Severity 5 – Immediate response, Targeted resolution within 8 business hours	
VIP/Executive User support	< 4 hours
Severity VIP – Immediate response, Targeted resolution within 4 hours (25 VIPs)	
Telephonic call logging – Answered within 40 seconds	> 80%
Calls dropped	< 2%
Email logging – Reference number issued	< 1 hour

Reference number issued – any channel	100%
With reference to the Telephony System, SLA for Monthly reporting on call volumes, call quality, outages, and SLA adherence and resolution (e.g., priority 1 faults resolved within 4 hours).	

—oOo—