



**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_A
Advert Date	27 March 2026
Issuer	South African National Parks
Closing Date and Time	04 May 2026 at 11H00

TABLE OF CONTENTS

1	DISCLAIMERS	3
2	THE BIDDING SELECTION PROCESS	3
3	REASONS FOR DISQUALIFICATION	9
4	INTRODUCTION TO SANPARKS	9
5	BUSINESS UNIT RESPONSIBLE FOR THE BID	11
6	CONTEXT OF THIS PROCUREMENT	12
7	CAPABILITIES	12
8	STRUCTURE	12
9	CONTRACT PERIOD	12
10	SPECIFICATIONS/SCOPE OF WORK.....	13
10.1	Core Services	14
10.2	LAN/WAN	25
10.3	Additional Services Required	32
10.4	Security Services	36
10.5	Additional Services.....	43
10.6	Additional Criteria to be Noted	45

1 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 permitted by law, SANParks shall 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 or any misinterpretation of this document. SANParks makes no representation, warranty, assurance, guarantee, or endorsement to any provider or Bidder concerning this document, whether regarding its accuracy, completeness or otherwise, and SANParks shall have no liability towards Bidders 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 bid 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 manipulation of bid outcomes.

SANParks reserves the right to amend, withdraw and/or cancel this bid at any time.

2 THE BIDDING SELECTION PROCESS

The evaluation process will be conducted in various phases. To progress to the next phase of evaluation, the Bidder must have fully complied with the requirements of the preceding phase. No allowance will be made for non-submitted documents, missing proof, or late submissions. If a Bidder's response is incomplete, the 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 "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):**

Bids that meet the functionality threshold under Phase 2 will be evaluated in terms of price and specific goals using the applicable preference point system prescribed by the Preferential Procurement Regulations 2022. Points will be allocated for price and for specific goals as detailed in the SBD forms and preference point system applicable to this bid.

Based on the outcome of the bid evaluation phases, the Bid Evaluation Committee will make recommendations to the Bid Adjudication Committee for 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 and signed by both parties.

Financial Due Diligence

Bidders will be subjected to a comprehensive financial review to assess their financial stability and capacity to deliver the required services. This review will focus on establishing the financial credibility, liquidity, and overall sustainability of the Bidders.

The Bidder is required to provide information regarding its financial status, supported by copies of the most recent three (3) years of **independently reviewed or audited** Annual Financial Statements or Annual Reports.

- **Phase 1: Mandatory Evaluation Criteria**

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

Failure to comply with 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.

- (1) The Bidder must hold a valid ICASA Electronic Communications Network Service (ECNS) and Electronic Communications Service (ECS) licence **OR** demonstrate a formal contractual relationship with a licensed telecommunications partner that holds the required ICASA licences. Where the Bidder relies on such a partner, the proposal must clearly identify the licensed entity and provide evidence of the relationship through a binding partnership agreement or letter of commitment. The Bidder must provide evidence of its relationship with the licence holder.
- (2) The main Bidder must demonstrate that they are a Microsoft Solution Partner with capability in Modern Work and Security. Proof of the certification from Microsoft must be provided.

SANParks acknowledges that Microsoft designations may change from time to time. The requirement is assessed at the bid closing date as an objective and independently verifiable threshold of current Microsoft competency based on the importance of Microsoft technologies in SANParks operations. Contract management provisions will include ongoing performance monitoring through SLA compliance, and SANParks reserves the right to include designation maintenance as a contract obligation to ensure ongoing competency throughout the contract term. This will be addressed during contract negotiation with the successful Bidder.

(3) The main Bidder must submit a valid and current COIDA Letter of Good Standing (LOGS) (not older than six (6) months at bid closing date) issued by the Compensation Fund of the Department of Employment and Labour.

(4) The Bidder must demonstrate they have a contractual relationship with at least two (2) data centre facilities located within the Republic of South Africa to separately support the production and disaster recovery environments required for the duration of this contract.

Bidders must also provide evidence of the data centre holding the following minimum certifications/attestations:

Tier III or equivalent for both production and disaster recovery environments.

Bidders may rely on subcontractors or consortium members to meet the data centre operational requirements, provided that such arrangements are supported by binding agreements.

(5) The main Bidder must 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; and
- e. PCI DSS.

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

Note: Where the Bidder relies on compliance with ISO/IEC 27017, the Bidder must hold a valid ISO/IEC 27001 certification issued by an accredited and authorised certification body, and such compliance must be either (i) expressly included within the scope of the ISO/IEC 27001 certification, or (ii) supported by a separate written attestation issued by a relevant certification body or auditor confirming assessment against ISO/IEC 27017 controls. Internal alignment, self-assessment, or self-declaration shall not be accepted as evidence of compliance.

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

- **Phase 2: Technical/Functional Evaluation Criteria**

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

- (1) Qualification 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 specified.
- (3) SANParks reserves the right to request a demonstration or platform access (with anonymised data) during its due diligence processes.

NO.	FUNCTIONALITY CRITERIA	WEIGHTING (%)	MAXIMUM TO BE AWARDED
1.	<p>Ability to provide the services by FSEs at all the identified sites</p> <p>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-A Annexures Excel Spreadsheet to capture the locations of FSEs.</p>	20	<p>20 = Support engineers less than 1 hour from site.</p> <p>16 = Support engineers from 1 hour but less than 2 hours from site.</p> <p>12 = Support engineers from 2 but less than 4 hours from site.</p> <p>8 = Support engineers from 4 hours but less than 6 hours from site.</p> <p>4 = Support engineers from 6 hours but less than 8 hours from site.</p> <p>0 = Support engineers 8 or more hours.</p>
2.	<p>Managed Services experience</p> <p>Please provide evidence of experience in managing services, associated contracts and vendors.</p> <p>Please provide the references on the client's letterheads, with the following information included:</p> <ul style="list-style-type: none"> • 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 • Start and end dates of the services that were provided to the client <p>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 letter.</p>	10	<p>5 = Experience has been shown in all 5 of the managed services.</p> <p>0 = Experience has not been demonstrated in all 5 of the managed services.</p> <p>If 0 points has been allocated above, then no points will be allocated for experience.</p> <p>Where 5 points has been allocated for the above, points for experience will be evaluated and allocated as follows:</p> <p>5 = Average of 5 years or more experience across all managed services.</p> <p>4 = Average of at least 4 years' experience but less than 5 years' experience across all managed services.</p> <p>3 = Average of at least 3 years' experience but less than 4 years' experience across all managed services.</p> <p>2 = Average of at least 2 years' experience but less than 3 years'</p>

NO.	FUNCTIONALITY CRITERIA	WEIGHTING (%)	MAXIMUM TO BE AWARDED
	<p>If any of the above information is missing, the reference letter will not be considered.</p> <p>Please cover the following managed services at a minimum:</p> <ul style="list-style-type: none"> • Front Office Services • Back Office Services • End User Services • ISP/Connectivity Services • Data Centre Management 		<p>experience across all managed services.</p> <p>1 = Less than 2 years but at least 1 year of experience across all managed services.</p> <p>0 = No evidence of experience provided.</p>
3.	<p>Capability</p> <p>The Bidder must provide the resource, with their relevant experience, certifications and qualifications as per Annexure 1G of the GNP-099-25-A Annexures Excel Spreadsheet.</p> <p>Bidders must also provide copies of CV's as well as all relevant certificates and qualifications.</p> <p>Any CV that is not accompanied by the relevant certification, will score 0.</p>	35	<p>35 points will be allocated if the average score equals or exceeds 80%.</p> <p>25 points will be allocated if the average score is between 70% and 79%.</p> <p>0 Points will be allocated if the average score is less than 70%.</p>
4.	<p>Ability of the Bidder in the management of endpoints</p> <p>Bidders must provide relevant evidence of ability in managing endpoints.</p> <p>Acceptable evidence includes either official client letters or a letter from the Original Equipment Manufacturer ("OEM") which includes the numbers of endpoints managed.</p>	5	<p>5 = ≥ 40000 endpoints managed.</p> <p>4 = < 40000 and ≥ 30000 endpoints managed.</p> <p>3 = < 30000 and ≥ 20000 endpoints managed.</p> <p>2 = < 20000 and ≥ 10000 endpoints managed.</p> <p>1 = < 10000 endpoints managed.</p> <p>0 = Bidder's endpoint managed capability does not exist.</p>
5.	<p>Ability in the management of servers</p> <p>Bidders must provide relevant evidence of ability in managing servers.</p> <p>Acceptable evidence includes either official client letters or a letter from the OEM which includes the numbers of servers managed.</p>	5	<p>5 = ≥ 4000 servers managed.</p> <p>4 = < 4000 and ≥ 3000 servers managed.</p> <p>3 = < 3000 and ≥ 2000 servers managed.</p> <p>2 = < 2000 and ≥ 1000 servers managed.</p> <p>1 = < 1000 servers managed.</p> <p>0 = Bidder's server management capability does not exist.</p>

NO.	FUNCTIONALITY CRITERIA	WEIGHTING (%)	MAXIMUM TO BE AWARDED
6.	<p>Ability in the management of databases</p> <p>Bidders must provide relevant evidence of ability in managing databases.</p> <p>Acceptable evidence includes either official client letters or a letter from the OEM which includes the number of databases managed.</p>	5	<p>5 = ≥ 2000 databases managed.</p> <p>4 = < 2000 and ≥ 1000 databases managed.</p> <p>3 = < 1000 and ≥ 500 databases managed.</p> <p>2 = < 500 and ≥ 250 databases managed.</p> <p>1 = < 250 databases managed.</p> <p>0 = Bidder's database management capability does not exist.</p>
7.	<p>Ability in Disaster Recovery as a Service (DRaaS)</p> <p>Bidders must provide relevant evidence of ability in DRaaS capabilities.</p> <p>Acceptable evidence includes either official client letters or a letter from the OEM which includes the number of protected workloads.</p>	10	<p>10 = The DRaaS capability is ≥ 10000 workloads.</p> <p>8 = The DRaaS capability is ≥ 9000 but < 10000 workloads.</p> <p>6 = The DRaaS capability is ≥ 8000 but < 9000 workloads.</p> <p>4 = The DRaaS capability is ≥ 7000 but < 8000 workloads.</p> <p>2 = The DRaaS capability is ≥ 5000 but < 7000 workloads.</p> <p>0 = Bidder's DRaaS capability does not exist.</p>
8.	<p>Cloud Interconnect Presence</p> <p>Bidders must provide relevant experience in implementing and operating interconnects with the following major global public cloud providers in South Africa:</p> <p>Amazon Web Services</p> <p>Microsoft Azure</p> <p>Google Cloud</p> <p>A maximum of two points will be allocated where Bidders show experience in other public cloud providers other than those listed above.</p> <p>Acceptable evidence includes either official client letters or a letter from the above providers.</p>	10	<p>10 = Experience in implementing or operating interconnects to all 3 specified cloud platforms.</p> <p>8 = Experience in implementing or operating interconnects to any 2 specified cloud platforms.</p> <p>6 = Experience in implementing or operating interconnects to 1 specified cloud platform.</p> <p>2 = Experience in implementing or operating interconnects in other cloud platforms.</p> <p>0 = No evidence of experience in any cloud platform provided.</p>

3 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 disqualification may take place without prior notice to the Bidder:

- Bidders whose tax matters are not in order (Instruction Note 09 of 2017/2018 Tax Compliance Status will apply).
- Bidders who are not registered on National Treasury's Central Supplier Database.
- 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 and 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 make 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.

4 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 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.

5 BUSINESS UNIT RESPONSIBLE FOR THE BID

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 EAD 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
Sage VIP Payroll and Premier HR
Memex
SANParks Reservation System, (will replace RoomSeeker)
NAC-Forescout
BizAzure Integration Services
Proofpoint- Security Awareness

6 CONTEXT OF THIS PROCUREMENT

South African National Parks (SANParks) invites prospective 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 into negotiations with the successful Bidder for the purposes of concluding a binding contract, inclusive of supporting schedules 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 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.

7 CAPABILITIES

- Manage Service Integration Governance;
- Manage the Service Integration Organisation;
- Manage Tools and Information;
- Manage Providers and Contracts; and
- Manage End-to-End Services.

8 STRUCTURE

- Prime-Vendor Approach.

9 CONTRACT PERIOD

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

10 SPECIFICATIONS/SCOPE OF WORK

SANParks is seeking the following services from Bidders 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 each service themselves or identify the sub-contractor responsible for delivering the service. The Bidder must perform the material portion 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 Identity and Financial Integrity
 - 10.6.4 Performance Criteria
 - 10.6.5 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. The transition period to the appointed Bidder is estimated to be 90 (ninety) days.

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 10.6.5 - 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. In addition, SANParks requires the SSA to ensure the continuous presence of a Service Delivery Manager on-site in Pretoria, with a suitably empowered delegate available to make decisions whenever the Service Delivery Manager 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 and Service Delivery Model 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 has 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 for 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 follow-up of incidents through their lifecycle to final resolution.

Logged incidents may not be pended without express permission from 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 regarding the service desk solution-

- licensing for up to 15 SANParks support staff to manage incidents assigned to them;
- the ability to provide 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 the Bidder's system into the SANParks data warehouse on MS SQL so that SANParks has access to the data for its own use and analysis in addition to what would be provided by the Bidder;
- the ability to provide comprehensive problem management, knowledge management, event management, request fulfilment, and task management; and
- SANParks has approximately 35 support calls per month relating to application support.

10.1.3 User Support

SANParks operates in a geographically dispersed environment across South Africa (refer to **Annexures 1K** and **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) (24/7 availability required)	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. Bidders are responsible for their own travel and accommodation costs for FSEs.

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 of location and FSE details.

The successful Bidder will be responsible for the following-

- 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, 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 10.6.5 - Service Levels Required.

Proposal Requirements-

Your proposal must address the following requirements—

- **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, etc.);
- **Network monitoring and 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 details 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 products, 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, whether on-premises 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 perspective and logging of all administrator-level user actions.

The services required must relate to the proactive 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 should note that the number of virtual machines indicated in the annexure is indicative only and is subject to change.

Please note the following requirements regarding server management-

- Server availability (>99%) with 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 or all cloud infrastructure, software, and platforms;
- Quarterly capacity planning is performed where applicable
- Full configuration and 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, and 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 an experienced SQL database administrator service that must ensure the database environment is configured per best practices, is secure and managed proactively. Databases must be maintained in a current state in consultation with application owners. Services must encompass ITIL® fully.

When performance issues are experienced, the problem must be subject to focused 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 operations and users.

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

The following needs to be addressed-

- 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 or all cloud-based databases for IaaS and PaaS deployments;
- Monthly capacity planning is performed where applicable;
- Full configuration and setup documentation of all databases with emphasis on security standards after or when changes occur;
- Database performance optimisation
- Disaster recovery testing every quarter; and
- Daily backup of databases.

10.1.8 Disaster Recovery Management

Business continuity is paramount to the ICT services provided to SANParks' operations. In particular, tourism operations cannot 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 Bidder 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 with the existing infrastructure, enabling swift failover to alternate resources, minimising downtime, and safeguarding the continuity of SANParks' mission-critical operations.

SANParks requires the Bidder 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, in addition to 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 the 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 or 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. Please refer to **Annexure 1M** - Backup & Recovery RTO & RPO in the GNP-099-25-A Annexures Excel Spreadsheet;
- 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 restoration 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.

- Please note that data backups must be retained for a period of 90 days in accordance with SANParks policies. SANParks' current backup capacity is estimated at 450 TB; however, this is dynamic and subject to change.

10.1.8.2 *Supported Workloads*

- Virtual: VMware vSphere, Microsoft Hyper-V, Other;
- Databases: Microsoft SQL Server, Oracle, MySQL, or other platforms;
- Cloud: AWS, Azure, Google Cloud, Microsoft 365, and VMware Cloud on AWS;
- SaaS: Microsoft 365 (Exchange, OneDrive, SharePoint, Teams), and other platforms;
- Kubernetes: Centralised protection and management; and
- File systems and 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 unauthorised 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 centre 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, and 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) and 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 its email archive cloud service 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 with 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 on the Mimecast service. This user count may change during the term of this contract, and the Bidder 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 the change management process;
- Perform any requested data extract as reasonably requested from time to time;
- Manage Mimecast 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 Bidder 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. 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);
- Automated patch discovery: Continuous scanning to detect missing patches and vulnerabilities across the environment;
- Prioritisation and Risk Scoring: Intelligent prioritisation 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 or 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 cost elements-

- 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 as follows-

- 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 or radio connections); and
- The price shall exclude the cost for LAN extensions to separate buildings or sites on the same premises via fibre or radio link.

10.2.1.2 *Expansion of the LAN*

This service should be costed into your proposal with the following base requirements-

- Armoured fibre must be used for fibre connections due to environmental issues;
- Bidders must use multimode fibre (distances will be a maximum of 1,000m);
- 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 and installation needs. Where SANParks is unable to provide accommodation, the Bidder must include such costs in the quotation, in line with the National Treasury Travel Guidelines for Government Institutions, published on the National Treasury's website from time to time.

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 Bidder 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 those locations specified in **Annexure 1F - WAN Pricing** of the GNP-099-25-A Annexures Excel Spreadsheet 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 network service providers and any other relevant providers.

The provisioning of last mile connectivity does not necessarily have to be by the same service provider, but the main service provider (the 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 VSAT has not been successful due to high latency, contention, and cost. SANParks would prefer VSAT to 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 two-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 Bidder 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 an SD-WAN network with connectivity back to a data centre that meets the requirements as specified in the mandatory criteria as well as local internet breakout for each site.

SANParks requires 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, and broadband). SD-WAN monitors link health (latency, jitter, and 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, and video conferencing) to prioritise critical workloads and avoid congestion;
- Security integration: SD-WAN can embed next-generation 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 or satellite) with minimal disruption.

Management of internet access should also be read together with security services as described under Section 10.4.

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. While Microsoft Teams Calling is the preferred platform (as SANParks currently subscribes to Microsoft 365 E5 licences), 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 or 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-premises 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;
- Provision of user support for 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, and mobile simultaneously);
- The 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 or 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 or 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 general business telephony solution) which meets the following requirements-

Inbound Call Handling-

- Skill-based routing, IVR selection, or customer history routing;
- Automatic Call Distribution (ACD) to available agents;
- Call transfer between agents or queues;
- Multi-queue capability (agents can join or leave multiple queues);
- Call overflow and interflow handling;

- Call queuing with estimated wait time announcements and queue position notifications; and
- Callback 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, and coaching);
- Live monitoring of calls and agent performance;
- Real-time dashboards and wallboards;
- Remote ability to log agents in or out for workforce management;
- Performance KPIs (AHT, FCR, service level adherence, abandonment rate, etc.);
- Quality management and evaluation tools;
- Workforce management integration (scheduling, forecasting, and adherence);
- Comprehensive logging of all supervisor actions (e.g., call monitoring, barging, recording access, agent adjustments, and 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 or missed calls, overflow or interflow calls, ACD vs non-ACD calls, and short handle calls;

- Custom report builder with export to PDF, Excel, and CSV;
- Automated and scheduled report distribution; and
- First login and 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 or PII compliance;
- Retention controls to ensure recordings comply with legal and regulatory requirements; and
- Retention of call recordings for a minimum of 5 years, 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. 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 or 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, including measures to prevent blacklisting of the 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 the 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 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 SMS solution, including how usage will be managed and billed to SANParks.

Describe the proposed opt-out function that will be provided and explain how 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 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*

SANParks already has existing infrastructure hosted within Teraco facilities. SANParks is currently running its own infrastructure at Teraco together with its IaaS environment, and the present internet breakout is also terminated at Teraco, which facilitates business integration. 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 Bidder will be required to-

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

10.3.3.1.2 The Bidder must migrate the existing private cloud workloads (refer to **Annexure 1D – Private Cloud Pricing**) to a new private cloud, which can be located at Teraco or at a data centre that meets the requirements as specified in the mandatory criteria;

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 as per point 10.1.1.1.2 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 environment from the current Cloud Maturity Model (CMM) level 1 (CMM 1 – Ad hoc) to CMM level 5 (optimised and proactive)-

- The cloud environment must comply with PCI DSS;
- The cloud environment must comply with 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 service model; and
- The immediate cloud requirements that must be catered for are 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 integration 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.

At a core, foundational level, the following must be considered and included-

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 currently running and hosted in the Azure tenant.

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

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

All servers in the E-Business web environment 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 Trust 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.

At 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 the security and integrity 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 Auditor General 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, including monitoring capacity, traffic, load, and performance impacts.

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

At a code and application level, support includes—

Ad-hoc and additional development of new systems, enhanced systems, mobile applications (linked to the SANParks web environment), APIs (server and/or client).

Development of, or assistance with components of development for, RESTful APIs or SOAP services.

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

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 setting up of UAT/SIT and change management of all web-related projects.

The skills and expertise relevant and preferable for the support of the SANParks website-

- Expert knowledge of Linux Operating Systems (CentOS);
- At least 5 years' experience in system administration and technical support on Linux systems with high-level proficiency in scripting, bash, and setting up and maintaining a LAMP, LNMP, or 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 integration 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 administrators, 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 objectives—

- 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 Security Operations Centre (SOC) Services

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 at SANParks;
- These events or incidents must be reported to the appropriate governance structure in SANParks;
- These events or 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 its 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 the following—

- 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 in 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 scanning 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 improve SANParks' security posture, enhance secure remote access, and protect both internal and public-facing systems.

The solution must 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 demonstrate how their service integrates with SANParks' incident response procedures and SOC operations.

The solution must 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 locally 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 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 support the following minimum requirements-

- 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 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 sanitisation;
- Malware detection, backdoor or 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 per month);
- Daily review of high-risk alerts;
- New plugin or security change reviews; and
- All services must be delivered as fully managed by the Bidder.

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 (e.g., 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, focusing on the skills they will bring to bear and previous experience in this regard.

Annual PCI DSS Recertification of SANParks-

- The Bidder shall be responsible for ensuring that SANParks undergoes annual PCI DSS recertification at the level required for its operations;
- The Bidder 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 Bidder 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 Bidder 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 Bidder shall assist SANParks in developing and implementing a remediation plan; and
- The Bidder is responsible for tracking remediation to closure and ensuring any follow-up validation required for PCI DSS compliance is completed.

Ongoing Compliance Support-

- The Bidder must provide SANParks with guidance, monitoring, and advisory services throughout the year to ensure continuous PCI DSS 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 may be carried forward 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 value-add services that align with SANParks' operational needs.

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;
- SANParks may not utilise these services every month, quarter, or year and will only be billed for hours spent on each assignment; and
- Any unused hours from any period may be carried forward to the next period.

10.5.1 ICT Maturity and Innovation Services

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 seeks to capitalise on proven technologies to improve its product offerings and supporting ICT environment. Together with improvements 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 with first-world communication challenges. Added to this are the prescripts relating to the natural environment and sense of place that may require Environmental Impact Assessments and/or Environmental Management Plans when infrastructure is required to be added to areas under management in accordance with 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 expand its knowledge of SANParks, its business and 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 bear regarding similar assignments, including relevant skills, qualifications, and capability.

The successful Bidder will be expected to attend an annual workshop with SANParks to review the growth or scaling back of the infrastructure and to assist in facilitating budgeting requirements for the year ahead. The successful Bidder will continually keep SANParks updated regarding asset management of the infrastructure.

10.5.2 Quality Assurance

SANParks requires the successful Bidder to assist its 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, policies, procedures, and operations;
- Select suitable and agile frameworks and standards in line with SANParks' strategies and business model;
- Propose and advise on governance model and organisational structure;
- Draft a set of policies and procedures for efficient and optimum processes and operations;
- Provide a brief implementation roadmap, including induction sessions for senior management and the 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 organisation to the IT strategy and document this using various architectural models or views that show how the current and future needs of the organisation 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 organisation's 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 and applications, eliminate or reduce software and process inefficiencies, increase productivity, and create new functionalities that benefit SANParks' operations.

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 sites. Refer to 4 for a listing of the SANParks sites as well as maps indicating their different locations.

Proposals should indicate clearly, amongst other matters, the capacity and capability they currently have geographically regarding-

- Human resources and staff complement;
- Location of dedicated staff, offices, or sub-contractors from where the sites will be serviced, considering the proposed service level requirements; and
- Where capacity at a site does not 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 by documenting the following-

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

10.6.3 Identity and Financial Integrity

Bidders are required to provide the following information-

- Financial information for each entity forming part of the bid must be provided;
- Summary of South African human and other resources and capacity;
- Summary of global human and other resources and capacity, if any;
- List of legal actions instituted by or against the Bidder for more than R1 million in the last three years; and
- Other information to support criteria as listed above.

10.6.4 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 (SLAs). 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.

10.6.5 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).	
