

NATIONAL HOME BUILDING



Terms of Reference



REQUEST FOR PROPOSALS FOR THE APPOINTMENT OF SUITABLE QUALIFIED SERVICE PROVIDERS TO PROVIDE MANAGED INFRASTRUCTURE SERVICES TO THE NHBRC FOR A PERIOD OF TWO (05) YEARS

RFP NO.:

NHBRC 08/2026

CLOSING DATE:

02 OCTOBER 2026

TIME:

11:00

SUBMISSION

<https://www.etenders.gov.za>

VIRTUAL NON-COMPULSORY HYBRID BRIEFING SESSION

<https://teams.microsoft.com/meet/362252380611593?n=A3aKrMazn1s4n>

DATE: 11 September 2026

TIME: 11:00

VENUE: ONLINE

1.1. This Request for Proposal (RFP) has been compiled by the NHBRC, and it is made available to the Bidders on the following basis.

1.2. Bidders submitting a Bid in response to this RFP are deemed to do so on the basis that they acknowledge and accept the terms and conditions set out below:

- a) The Bidder must be registered on the National Treasury's Central Supplier Database ("the CSD") and ensure that, if it is successful, it remains so registered and further ensure that the information on the CSD is up-to-date for the duration of the contract.
- b) The Bidder must ensure that it is tax compliant at the time of submitting its bid in response to this RFP, and if it is successful, it remains tax compliant for the duration of the contract. In this regard, the Bidder undertakes to provide the NHBRC with a Tax Clearance Certificate issued by the South African Revenue Services ("SARS") on an annual basis, confirming that it is tax compliant.
- c) The NHBRC reserves the right to amend, modify or withdraw this RFP or amend, modify or terminate any of the procedures or requirements set out herein at any time (and from time to time), without prior notice and without liability to compensate or reimburse any person.
- d) If the NHBRC amends this RFP, the amendment will be sent to each Bidder in writing or publicized as the case may be. No oral amendments by any person will be considered or acknowledged.
- e) The NHBRC reserves the right to carry out site inspections or call for supporting documentation in order to confirm any information provided by a Bidder in its RFP Bid.
- f) This RFP is not intended to form the basis of a decision to enter into any transaction involving the NHBRC and does not constitute an offer or recommendation to enter into such transaction, or an intention to enter into any legal relationship with any person.
- g) A Bid submitted in response to this RFP will constitute a binding offer which will remain binding and irrevocable for a period of ninety (90) days from the date of submission to the NHBRC. The offer constituted by the Bid will be deemed not to have been accepted and no agreement will be deemed to be reached with any Bidder, unless and until a binding Agreement and other related transactions/documents are concluded between the NHBRC and the Preferred Bidder.
- h) The distribution of this RFP outside the Republic of South Africa may be restricted or prohibited by the laws of other countries. Recipients of this RFP are advised to familiarize themselves with and comply with all such restrictions or prohibitions applicable in those jurisdictions, and neither the NHBRC nor any of their respective directors, officers, employees, agents, representatives or advisors, accepts liability to any person for any damages arising out of or in connection with the breach of any restriction or provision outside the Republic of South Africa. Persons contemplating submitting a Bid are advised to obtain legal advice as to the possible consequences thereof in terms of the law of the jurisdictions in which they are located.
- i) Recipients of this RFP document may only distribute it to other parties whom they wish to involve as part of their Bidder consortium in submitting a Bid.
- j) Neither the NHBRC nor any of their respective directors, officers, employees, agents, representatives or advisors will assume any obligation for any costs or expenses incurred by any party in or associated with preparing or submitting a Bid in response to the RFP.

- k) No entity may be involved, whether directly or indirectly, in more than one Bid in response to this RFP. Failure to comply with this requirement may, within the sole discretion of the NHBRC, result in disqualification of the relevant entity.
- l) Any material change in the control and/or composition of any Bidder or any core member of a Bidder after submission of a Bid shall require the prior written approval of the NHBRC, and any failure to seek such approval from the NHBRC shall result in the NHBRC being entitled, in its sole discretion, to disqualify the relevant Bidder from any further participation in the Bid process. The NHBRC shall be the sole arbiter as to what constitutes a “material change in the control and/or composition of any Bidder”, and as to what constitutes a “core member of a Bidder” for purposes of such approval. Any request for such approval shall be made to the NHBRC’s Supply Chain Management (“SCM”) in writing and shall provide sufficient reasons and information to allow the NHBRC to make a decision. The NHBRC reserves the right to accept or reject any such request for approval at its sole discretion.
- m) Briefing Session: There will be a non-compulsory hybrid briefing session. The sharing of information and clarifications of issues related to this Bid, as given by the NHBRC will form part of this Bid and responses.
- n) Any requirement set out in this RFP that stipulates the form and/or content of any aspect of a Bid, is stipulated for the sole benefit of the NHBRC, and save as expressly stated to the contrary, may be waived by the NHBRC in its sole discretion at any stage in the RFP process.
- o) The NHBRC and its advisors shall rely on a Bid as being accurate and complete in relation to the information and proposals provided therein by the Bidders.
- p) All Bids submitted to NHBRC will become the property of the NHBRC and will as such not be returned to the Bidder. The NHBRC will make all reasonable efforts to maintain proposals in confidence. Proprietary information should be identified as such in each proposal.
- q) The bid submitted by the Bidder shall be considered irregular if it shows any omissions, alteration of form, additions, or conditions not called for, or irregularities of any kind. However, the NHBRC reserves the right to waive any irregularities and to make an award in the best interest of the company.
- r) The NHBRC reserves the right to accept or reject the Proposal.
- s) RFPs shall be rejected, among other reasons, where Bids are received after the closing date and time as specified in the RFP.
- t) Potential service provider(s) shall be disqualified and their Bids not considered among other reasons, for any of the following specific reasons:
 - a) If the SCM Mandatory Documents are not submitted and completed as per this RFP; and/or
 - b) The Bid contains irregularities.
- u) The NHBRC reserves the right to require that any bidder provide a formal presentation of its RFP at a date and time to be determined by the NHBRC. The NHBRC shall provide all instructions and clarification regarding the purpose and scope of the presentation. All expenses must be borne by the bidder.
- v) All costs associated with the preparation and submission of the Bid are the responsibility of the Bidder. The costs shall not be chargeable to the NHBRC by successful or unsuccessful Bidder.
- w) This document is released for the sole purpose of responding to this RFP and must be considered confidential. In addition, the use, reproduction or disclosure of the requirements, specifications or other material in this RFP is strictly prohibited.
- x) All Bids must be formulated and submitted in accordance with the requirements of this RFP.

2. ABOUT THE NHBRC

2.1. The National Home Builders Registration Council (NHBRC) is a regulator established in terms of section 2 of the Housing Consumers Protection Measures Act 95 of 1998 ("the Act"). Section 3 of the Act provides that the objects of the NHBRC are to:

- represent the interests of housing consumers by providing warranty protection against defects in new homes;
- regulate the home building industry;
- provide protection to housing consumers in respect of the failure of home builders to comply with their obligations in terms of this Act;
- establish and promote ethical and technical standards in the home building industry;
- improve structural quality in the interests of housing consumers and the home-building industry;
- promote housing consumer rights and to provide housing consumer information;
- communicate with and to assist home builders to register in terms of this Act;
- assist home builders, through training and inspection, to achieve and maintain satisfactory technical standards of home building;
- regulate insurers contemplated in section 23 (9) (a); and
- in particular, achieve the stated objectives of this section in the subsidy housing sector.

The Council is furthermore empowered by the Act:

- "to engage in undertakings to promote improved structural quality of homes constructed in the Republic;
 - "to engage in undertakings to improve ethical and technical standards in the home building industry;
 - "to keep a record of competent persons"; and
 - "to generally do all things necessary or expedient to achieve its objectives and the objectives of this Act."
- a) The NHBRC's primary mandate is to manage the risk of structural defects in the home building industry and in so doing, protect the consumer. A prime activity of the NHBRC is to manage its risk exposure in terms of the warranty scheme, in order to ensure that it is not unduly exposed to claims. The current risk management tools being used by the Council include the Registration of Home Builders, enrolment and inspection of homes, the Home Building Manual which incorporates designs and construction rules, and the appointment of competent persons by the Home Builder to perform certain tasks.
- b) The NHBRC's goal is to ensure capital preservation to ensure it remains financially viable to meet claims as they arise and that no recourse to the Minister of Human Settlements for additional funds is necessary at any time in terms of section 17(3)-(5) of the Act.
- c) The annual actuarial report is required in terms of the Housing Consumers Protection Measures Act, to value the actuarial liabilities of the NHBRC's warranty fund.
- d) The investment strategy should be implemented with due regard to the liabilities of the NHBRC, the nature of the funds in general, Solvency Assessment and Management (SAM) and the low-risk tolerance and return requirements of the Council.

3. NHBRC OFFICES

3.1. The NHBRC is a medium-sized organization with a staff complement of approximately 544 employees. The NHBRC's Head Office is located in Sunninghill, Gauteng, with nine (09) Provincial Offices of varying size and 12 Satellite Offices which are located in the following areas:

NHBRC OFFICE LOCATIONS		NHBRC OFFICE LOCATIONS	
1	Head Office, (Sunninghill)	13	Eastern Cape (East London) - Satellite
2	Gauteng (Sunninghill) – Provincial	14	Western Cape (George) - Satellite
3	Kwa-Zulu Natal (Durban) – Provincial	15	North West (Klerksdorp) - Satellite
4	Western Cape (Cape Town) – Provincial	16	Limpopo (Tzaneen) - Satellite
5	Eastern Cape (Port Elizabeth) – Provincial	17	Limpopo (Modimolle) - Satellite
6	North West (Rustenburg) – Provincial	18	Mpumalanga (Witbank) - Satellite
7	Limpopo (Polokwane) – Provincial	19	Free State (Bethlehem) – Satellite
8	Mpumalanga (Nelspruit) – Provincial	20	North West (Mafikeng) – Satellite
9	Free State (Bloemfontein) – Provincial	21	Limpopo (Thulamela) – Satellite
10	Northern Cape (Kimberly) - Provincial	22	Gauteng (Pretoria) – Satellite
11	Kwa-Zulu Natal (Newcastle) - Satellite	23	Eric Molobi Innovation Hub (Soshanguve)
12	Kwa-Zulu Natal (Richards Bay) - Satellite		

4. INTRODUCTION

4.1. The National Home Builders Registration Council is mandated by the Housing Consumers Protection Measures Act, 1998 (Act No. 95 of 1998) to regulate the home building industry and protect housing consumers. The NHBRC ensures that it delivers on its mandate by delivering on its products and services, and the key performance indicators that are contained in the organizational scorecard.

VISION

To be the Champion of the Housing Consumers.

MISSION

To Protect the Housing Consumers and to Regulate the Homebuilding Environment.

MOTTO

Assuring Quality Homes.

STRATEGY OF NHBRC

The strategy of the NHBRC is based on the following pillars:

- To ensure that housing consumers and home builders are educated on their rights and obligations.
- To entrench a culture of compliance through fair and efficient enforcement mechanisms
- To research and introduce innovative products, methods and technologies within the homebuilding industry.
- To maintain a sustainable warranty fund

5. PURPOSE

- 5.1. The purpose of this document is to Request for Proposals (RFP) is to appoint a qualified service provider to deliver a fully integrated Managed Infrastructure Solution for NHBRC for a period of five (5) years.
- 5.2. The solution must support NHBRC's operational, regulatory, and digital transformation requirements through a secure, scalable, and resilient ICT environment.
- 5.3. The appointed service provider will assume end-to-end accountability for service delivery, performance, availability, and continuous improvement across all infrastructure components.

6. CURRENT ENVIRONMENT

6.1. CURRENT ENVIRONMENT

- 6.1.1. The NHBRC operates a hybrid ICT environment comprising on-premises infrastructure, managed hosting services, and cloud-based workloads hosted on Microsoft Azure.
- 6.1.2. The current hosting environment includes:
- **Eighteen (19) virtual machines hosted on Hyper-V infrastructure**
 - **One (1) Active Directory Domain Controller**
 - **A structured backup approach consisting of daily incremental, full weekly, and monthly archive backups, including off-site replication for disaster recovery purposes**
- 6.1.3. The proposed solution must seamlessly integrate these environments into a unified, secure, and scalable architecture, ensuring consistency across hosting, identity, backup, and disaster recovery services.

6.2. ENVIRONMENT SIZING AND SCALABILITY REQUIREMENTS

- 6.2.1. The solution must be designed based on the current baseline environment and must allow for growth over the contract period.
- 6.2.2. Server Spécifications:(Baseline)

Metric	Value
Total Servers	19
Total vCPU	106
Total RAM (GB)	860
Total Allocated / Provisioned Storage (GB)	41582,6
Total Allocated / Provisioned Storage (TB)	40,61
Total VMDK In-Use Storage (GB)	41329,7
Servers Powered On	14
Servers Powered Off	5
Storage Tier in Use	Silver (100% of allocated capacity)

6.3. SCALABILITY EXPECTATIONS

- 6.3.1. Horizontal and vertical scaling of compute, storage, and network resources
- 6.3.2. Allow rapid onboarding of new users, offices, applications, and digital services
- 6.3.3. Increased security and monitoring capacity
- 6.3.4. Elastic bandwidth and infrastructure scaling
- 6.3.5. Growth of at **least 20% per annum** without redesign

7. SCOPE OF WORK

7.1. OVERVIEW

- 7.1.1. The NHBRC requires a fully integrated, end-to-end managed infrastructure solution delivered under a single Service Provider model.
- 7.1.2. The appointed Service Provider shall be responsible for the design, implementation, integration, management, and continuous optimisation of all services within scope.
- 7.1.3. The solution shall cover the following service components:
 - a) Managed Hosting and Infrastructure (IaaS)**
 - b) Network and Connectivity Services**
 - c) Infrastructure Security and Monitoring**
 - d) Backup, Disaster Recovery and Business Continuity**
 - e) Unified Communications and Collaboration**
 - f) Service Management and Governance**
- 7.1.4. Bidders must propose a single, integrated solution across all service components.
- 7.1.5. The Service Provider shall act as the prime contractor and shall retain full accountability for all services, including those delivered through subcontractors, partners, or OEMs.
- 7.1.6. Where third-party providers are utilised, the Service Provider shall:
 - Ensure seamless integration across all service components
 - Remain fully accountable for service delivery, performance, and SLA compliance
 - Manage all subcontractors and OEMs as part of a unified delivery model
- 7.1.7. NHBRC shall maintain a single contractual and operational relationship with the appointed Service Provider.
- 7.1.8. The Service Provider shall ensure that the solution:
 - Aligns with NHBRC governance, risk, and compliance requirements
 - Supports asset ownership and exit management provisions
 - Provides transparent and cost-effective service delivery
- 7.1.9. The Service Provider shall be fully accountable for both technical and commercial performance throughout the contract lifecycle.

7.2. MANAGED HOSTING AND INFRASTRUCTURE-AS-A-SERVICE (IAAS)

7.2.1. The Service Provider shall deliver a secure, scalable, and resilient Infrastructure-as-a-Service (IaaS) environment aligned to NHBRC's hybrid ICT operations.

7.2.1.1. The solution shall:

- 7.2.1.1.1. Support current and future workloads (including SAP and business applications)
- 7.2.1.1.2. Enable hybrid and cloud-aligned architecture (including Microsoft Azure)
- 7.2.1.1.3. Ensure high availability and performance across all hosted environments

7.2.2. Data Centre Facilities

7.2.2.1. The Service Provider shall utilise enterprise-grade data centre facilities.

7.2.2.2. The data centre (primary site) must meet the following **minimum requirements**:

- 7.2.2.2.1. **Tier III certification** issued by the **Uptime Institute** or demonstrate compliance with an equivalent **TIA-942 Rated 3 Facility Certification standard**, to ensure high availability, redundancy, and operational resilience.
- 7.2.2.2.2. Located **within South Africa**, with geographic separation between primary and secondary site.
- 7.2.2.2.3. Provide environmental monitoring capabilities, including temperature, humidity, fire detection, and power conditions.
- 7.2.2.2.4. Include redundant power infrastructure (UPS and backup generators) to ensure continuous service availability and uninterrupted operations.
- 7.2.2.2.5. Support secure interconnectivity with major telecommunications providers and cloud platforms, including Microsoft Azure, Amazon Web Services, and Google Cloud, and must incorporate appropriate network segmentation measures, including Demilitarized Zones (DMZs), where applicable.
- 7.2.2.2.6. Implement robust physical security measures, including 24/7 surveillance, controlled access mechanisms, and continuous security monitoring.
- 7.2.2.2.7. Provide an appropriate infrastructure design, including raised flooring where applicable, structured cabling, and adequate power and cooling capacity to support both current operational requirements and future scalability needs.

7.2.3. Core Responsibilities

7.2.3.1. The Service Provider shall be responsible for:

- 7.2.3.1.1. Provision and management of enterprise-grade virtualised infrastructure (compute, storage, and networking)
- 7.2.3.1.2. Host and manage NHBRC systems and applications
- 7.2.3.1.3. Perform workload migration and optimisation
- 7.2.3.1.4. Manage operating system lifecycle (patching, updates, upgrades)
- 7.2.3.1.5. Monitoring infrastructure availability, performance, and capacity
- 7.2.3.1.6. Integration with Microsoft Entra ID (Azure AD) and other IAM services.
- 7.2.3.1.7. Support for hybrid architecture across on premises, hosted, and cloud environments

7.2.4. Architecture and Automation

7.2.4.1. The Service Provider shall implement automated and standardised infrastructure management practices.

7.2.4.2. This shall include:

7.2.4.2.1. Use of Infrastructure-as-Code (IaC) or equivalent automation tools

7.2.4.2.2. Automated provisioning, configuration, and scaling

7.2.4.2.3. Standardised configuration baselines

7.2.4.2.4. Automated patching and update processes

7.2.4.3. Manual processes must be minimised, and all critical operations must be repeatable, traceable, and auditable.

7.2.5. Cost Management and Optimisation

7.2.5.1. The Service Provider shall ensure efficient use of infrastructure resources.

7.2.5.2. This includes:

7.2.5.2.1. Monitoring resource consumption

7.2.5.2.2. Rightsizing compute and storage

7.2.5.2.3. Eliminating underutilised resources

7.2.5.2.4. Providing optimisation recommendations

7.2.5.3. The Service Provider shall deliver:

7.2.5.3.1. Monthly utilisation and cost reports

7.2.5.3.2. Recommendations for cost improvements

7.2.6. High Availability and Resilience

7.2.6.1. The solution shall be designed to meet SLA requirements and ensure service continuity.

7.2.6.2. This includes:

7.2.6.2.1. Redundancy across compute, storage, and network layers

7.2.6.2.2. Minimal single points of failure

7.2.6.2.3. Failover and recovery capabilities

7.2.7. Monitoring and Performance Management

7.2.7.1. The Service Provider shall provide continuous monitoring of infrastructure and applications. This includes:

7.2.7.1.1. 24/7 monitoring of availability and performance

7.2.7.1.2. Proactive alerting on service degradation

7.2.7.1.3. Real-time dashboards aligned to SLA reporting

7.2.7.1.4. Root cause analysis and incident reporting

7.2.8. Asset Ownership and Licensing Model

7.2.8.1. The bidder shall clearly define the ownership model for all components.

7.2.8.2. Ownership models may include Service Provider-owned, NHBRC-owned or Hybrid model

7.2.8.3. The proposal must

- 7.2.8.3.1. Clearly identify ownership of all key components, including compute, storage, networking, security platforms, software licensing, and management tools.
- 7.2.8.3.2. Ensure transparency in ownership, access, and control;
- 7.2.8.3.3. Remain accountable for all assets, regardless of ownership, including insurance.
- 7.2.8.3.4. Support seamless transition in line with exit management requirements; and
- 7.2.8.3.5. Avoid dependencies that may restrict NHBRC's operational or contractual flexibility.

7.2.9. Technology Refresh and Lifecycle Management

7.2.9.1. The Service Provider shall ensure that all technologies utilised in the solution remain vendor-supported for the duration of the contract.

7.2.9.2. The Service Provider shall:

- 7.2.9.2.1. Ensure all platforms, systems, and software remain within vendor support lifecycle periods
- 7.2.9.2.2. Proactively identify and recommend technology refresh or upgrades where required
- 7.2.9.2.3. Implements refresh activities to maintain performance, security, and supportability of the environment

7.3. NETWORK, CONNECTIVITY, AND SECURITY SERVICES

7.3.1. The Service Provider shall design, implement, and manage a secure, reliable, and high-performance network environment supporting all NHBRC locations and hosted services.

7.3.2. Wide Area Network (WAN) and Branch Connectivity

7.3.2.1. The Service Provider shall provide a resilient Wide Area Network (WAN) solution connecting all NHBRC sites.

7.3.2.2. The solution must:

- 7.3.2.2.1. Provide dual connectivity (primary and secondary) links per site
- 7.3.2.2.2. Ensure high availability
- 7.3.2.2.3. Support a cloud-aware Software-Defined Wide Area Network (SD-WAN) architecture or equivalent, capable of intelligent traffic routing and optimisation
- 7.3.2.2.4. Enable secure connectivity between branch offices, data centres, and cloud environments (e.g. IPSec or equivalent)
- 7.3.2.2.5. Provide Quality of Service (QoS) for prioritisation of Microsoft 365, Microsoft Teams voice and video, SAP and critical business applications
- 7.3.2.2.6. The proposed solution must align with the existing environment and include a migration approach where applicable.

7.3.3. Network Performance and Quality

7.3.3.1. The Service Provider shall ensure network performance supports business applications.

7.3.3.2. The solution must support:

- 7.3.3.2.1. Low latency for real-time services (e.g. voice and video)
- 7.3.3.2.2. Minimal packet loss and jitter for unified communications
- 7.3.3.2.3. Consistent bandwidth availability per site

7.3.3.3. The Service Provider shall monitor performance and resolve bottlenecks proactively.

7.3.4. LAN and Wireless Infrastructure

7.3.4.1. The Service Provider shall design and manage LAN and wireless infrastructure across all NHBRC sites.

7.3.4.2. This includes:

- 7.3.4.2.1. Enterprise-grade switching infrastructure
- 7.3.4.2.2. VLAN segmentation and access control
- 7.3.4.2.3. High availability design at core and access layers
- 7.3.4.2.4. Wireless access with secure authentication
- 7.3.4.2.5. Segmentation of user groups (corporate, guest, privileged)
- 7.3.4.2.6. Centralised management and monitoring

7.3.5. Network Security and Integration

7.3.5.1. All network services shall align with the infrastructure security requirements defined in Section 7.4.

7.3.5.2. The solution must Integrate with existing or proposed firewall environments

- 7.3.5.2.1. Support network segmentation, including DMZ design where required
- 7.3.5.2.2. Ensure visibility of network traffic

7.3.6. Monitoring and Reporting

7.3.6.1. The Service Provider shall provide end-to-end monitoring of network services. This includes:

- 7.3.6.1.1. Real-time monitoring of availability, performance, and utilisation
- 7.3.6.1.2. Proactive alerting and incident notification
- 7.3.6.1.3. SLA-aligned reporting
- 7.3.6.1.4. Perform ongoing capacity planning

7.3.7. Data Centre and DR Connectivity

7.3.7.1. The Service Provider shall ensure secure and reliable connectivity between primary and disaster recovery environments.

7.3.7.2. This includes Support replication traffic and failover operations

- 7.3.7.2.1. Ensure continuous access during disaster recovery scenarios
- 7.3.7.2.2. Align with defined DR requirements

7.3.8. Integration Requirements

7.3.8.1. All network services must operate as part of an integrated ICT ecosystem and interoperate seamlessly with:

- 7.3.8.1.1. Hosting and infrastructure services
- 7.3.8.1.2. Security services (Section 7.4)
- 7.3.8.1.3. Backup and disaster recovery solutions
- 7.3.8.1.4. Cloud and hybrid environments

7.4. INFRASTRUCTURE SECURITY AND MONITORING

7.4.1. The Service Provider shall implement and manage security controls to protect all infrastructure, platforms, and environments used to deliver services to the NHBRC.

7.4.1.1. The solution shall ensure the confidentiality, integrity, and availability of the NHBRC systems and data hosted within the Service Provider's environment.

7.4.2. Security Responsibility Model

7.4.2.1. The Service Provider shall be responsible for securing and monitoring the infrastructure under its control.

7.4.2.2. This includes Protection of hosted systems, platforms, and workloads

7.4.2.2.1. Monitoring of infrastructure, network, and platform-level security events

7.4.2.2.2. Detection and response to security threats within the hosting environment

7.4.2.3. The Service Provider shall ensure that all security capabilities integrate with NHBRC's current or future security operations, including any centrally managed Security Operations Centre (SOC).

7.4.3. Core Security Controls

7.4.3.1. The Service Provider shall implement and maintain the following:

7.4.3.1.1. Server and infrastructure hardening

7.4.3.1.2. Endpoint Detection and Response (EDR) or equivalent

7.4.3.1.3. Malware protection and threat prevention

7.4.3.1.4. Vulnerability scanning and patch management

7.4.3.1.5. Data encryption (at rest and in transit)

7.4.3.1.6. Network security controls aligned to approved architecture

7.4.3.2. All controls must be aligned with NHBRC security policies and industry best practices.

7.4.4. Minimum Security Control Requirements

7.4.4.1. The Service Provider shall implement and maintain, at a minimum, the following security controls throughout the contract duration:

7.4.4.1.1. Identity and Access Management

7.4.4.1.2. Multi-Factor Authentication (MFA) for all privileged and remote administrative access.

7.4.4.1.3. Role-Based Access Control (RBAC) aligned to the principle of least privilege.

7.4.4.1.4. Privileged Access Management (PAM) controls for privileged and administrative accounts.

7.4.4.1.5. Periodic access reviews and recertification of privileged accounts.

7.4.4.2. Infrastructure Protection

7.4.4.2.1. Secure configuration baselines aligned to recognised industry standards.

7.4.4.2.2. Endpoint Detection and Response (EDR) and/or Extended Detection and Response (XDR) capabilities.

7.4.4.2.3. Next-Generation Firewall (NGFW) protection.

7.4.4.2.4. Network segmentation and Zero Trust security principles.

7.4.4.2.5. Web Application Firewall (WAF) protection for internet-facing applications where applicable.

7.4.4.2.6. Distributed Denial of Service (DDoS) protection mechanisms.

7.4.4.3. Vulnerability Management

- 7.4.4.3.1. Quarterly authenticated vulnerability assessments.
- 7.4.4.3.2. Annual independent penetration testing.
- 7.4.4.3.3. Risk-based remediation of identified vulnerabilities.
- 7.4.4.3.4. Patch management aligned with agreed remediation timelines.

7.4.4.4. Data Protection

- 7.4.4.4.1. Encryption of data at rest and in transit.
- 7.4.4.4.2. Customer-controlled encryption keys where applicable.
- 7.4.4.4.3. Secure key management and rotation procedures.
- 7.4.4.4.4. Data Loss Prevention controls where applicable.

7.4.4.5. Supply Chain Security

- 7.4.4.5.1. Security due diligence of subcontractors and service partners.
- 7.4.4.5.2. Continuous monitoring of critical service providers.
- 7.4.4.5.3. Maintenance of an approved subcontractor register.

7.4.4.6. Assurance

- 7.4.4.6.1. The Service Provider shall annually provide evidence of independent security assurance assessments and remediation activities.

7.4.5. Security Monitoring and Event Management

7.4.5.1. The Service Provider shall:

- 7.4.5.1.1. Monitor systems, networks, and infrastructure for security events
- 7.4.5.1.2. Generate alerts for suspicious or malicious activity
- 7.4.5.1.3. Investigate and respond to incidents affecting hosted services
- 7.4.5.1.4. Timely detection and escalation of security events
- 7.4.5.1.5. Maintenance of incident logs and audit trails
- 7.4.5.1.6. Availability of security event data for analysis and reporting
- 7.4.5.1.7. Provide logs and telemetry to the NHBRC or third-party Security Operations Centre/Security Information and Event Management (SOC/SIEM) platforms
- 7.4.5.1.8. Enable integration with centralised monitoring systems

7.4.6. Vulnerability and Patch Management

7.4.6.1. The Service Provider shall implement continuous vulnerability and patch management processes, including:

- 7.4.6.1.1. Regular vulnerability scanning across all systems
- 7.4.6.1.2. Risk-based prioritisation and remediation of identified vulnerabilities
- 7.4.6.1.3. Timely application of security patches and updates

7.4.6.2. The Service Provider shall provide regular reports on:

- 7.4.6.2.1. Vulnerability status
- 7.4.6.2.2. Remediation activities
- 7.4.6.2.3. Compliance with patching requirements

7.4.7. Incident Management and Response

7.4.7.1. The Service Provider shall:

- 7.4.7.1.1. Detect and respond to security incidents within its environment
- 7.4.7.1.2. Escalate incidents to the NHBRC in accordance with agreed procedures
- 7.4.7.1.3. Support investigation, containment, and remediation activities
- 7.4.7.1.4. Maintain documented incident response procedures
- 7.4.7.1.5. Provide incident reports, including root cause analysis and corrective actions

7.4.8. Logging and Audit

7.4.8.1. The Service Provider shall implement centralised logging across all managed environments.

7.4.8.2. Logs must:

- 7.4.8.2.1. Capture system, network, and security events
- 7.4.8.2.2. Be time-synchronised and protected from tampering
- 7.4.8.2.3. Be retained in accordance with NHBRC requirements
- 7.4.8.2.4. Ensure logs are accessible for audit purposes
- 7.4.8.2.5. Be available for integration into external monitoring platforms

7.4.9. Reporting and Governance

7.4.9.1. The Service Provider should provide regular security reporting, including:

- 7.4.9.1.1. Security incidents and response actions
- 7.4.9.1.2. Vulnerability and patch compliance status
- 7.4.9.1.3. Security risks and trends

7.4.9.2. The Service Provider shall participate in the NHBRC governance structures related to security and risk management.

7.4.10. Compliance and Standards

7.4.10.1. The Service Provider shall ensure that all security controls and processes align with:

- 7.4.10.1.1. ISO/IEC 27001:2022 or ISO 22301:2019 or equivalent standards
- 7.4.10.1.2. POPIA requirements
- 7.4.10.1.3. NHBRC internal security policies

7.4.11. POPIA Operator Obligations

7.4.11.1. The Service Provider shall act as an Operator as contemplated in the Protection of Personal Information Act (POPIA).

7.4.11.2. The Service Provider shall:

- 7.4.11.2.1. Process personal information only on documented instructions from NHBRC.
- 7.4.11.2.2. Maintain strict confidentiality regarding all NHBRC information.
- 7.4.11.2.3. Ensure all personnel with access to NHBRC information are appropriately authorised.
- 7.4.11.2.4. Maintain an approved Sub-Operator Register identifying all subcontractors processing NHBRC information.
- 7.4.11.2.5. Obtain prior written approval from NHBRC before appointing any Sub-Operator.
- 7.4.11.2.6. Ensure all personal information remains hosted within the Republic of South Africa unless explicitly authorised by NHBRC.

- 7.4.11.2.7. Implement controls governing cross-border transfers of personal information.
- 7.4.11.2.8. Cooperate fully with NHBRC during security incidents, breach investigations, regulatory enquiries, and audit activities.
- 7.4.11.2.9. Notify NHBRC immediately upon becoming aware of an actual or suspected privacy or security breach.
- 7.4.11.2.10. Provide NHBRC with audit rights relating to the processing and safeguarding of personal information.
- 7.4.11.2.11. Support NHBRC in responding to data-subject requests and regulatory obligations.
- 7.4.11.2.12. Upon termination or expiry of the contract, return all NHBRC data in an agreed format and provide certified evidence of secure destruction of residual copies.

7.5. BACKUP, RESTORE, AND BUSINESS CONTINUITY

- 7.5.1. The Service Provider shall implement and manage a backup and disaster recovery solution to ensure the protection, availability, and recoverability of NHBRC systems and data.

7.5.2. Recovery Objectives

- 7.5.2.1. The Service Provider shall define and implement recovery targets aligned to business requirements.

Service Tier	RTO	RPO
Critical	4 hrs	15 min
Important	8 hrs	1 hr
Standard	24 hrs	24 hrs

- 7.5.2.2. This includes:

- 7.5.2.2.1. Defined Recovery Time Objectives (RTO) for system restoration
- 7.5.2.2.2. Defined Recovery Point Objectives (RPO) for data protection

7.5.3. Backup Services

- 7.5.3.1. The Service Provider shall:

- 7.5.3.1.1. Implement backup solutions across all environments
- 7.5.3.1.2. The backup approach must be daily incremental, full weekly, and a monthly archive
- 7.5.3.1.3. Perform regular backups of servers, databases, and application data
- 7.5.3.1.4. Ensure encryption of backup data at rest and in transit
- 7.5.3.1.5. Backups must:
 - Be monitored and verified regularly
 - Support restoration at file, system, and application levels

7.5.4. Backup Security and Resilience

- 7.5.4.1. The backup solution shall incorporate:

- 7.5.4.1.1. Immutable backup repositories.
- 7.5.4.1.2. Air-gapped or logically isolated backup copies.
- 7.5.4.1.3. Backup encryption at rest and in transit.

- 7.5.4.1.4. Backup integrity verification and automated validation processes.
- 7.5.4.1.5. Regular backup restoration testing.
- 7.5.4.1.6. Ransomware recovery capabilities.
- 7.5.4.1.7. Independent administrative credentials for backup environments.
- 7.5.4.1.8. A 3-2-1-1-0 backup strategy or equivalent.

7.5.4.2. Where 3 copies of data.

- 7.5.4.2.1. 2 different storage media.
- 7.5.4.2.2. 1 offsite copy.
- 7.5.4.2.3. 1 immutable or air-gapped copy.
- 7.5.4.2.4. 0 backup verification errors.

7.5.5. Disaster Recovery Architecture

7.5.5.1. The Service Provider shall provide a Disaster Recovery environment which:

- 7.5.5.1.1. Is located within South Africa.
- 7.5.5.1.2. Is geographically separated from the primary site.
- 7.5.5.1.3. Utilises separate utility infrastructure and power grids where possible.
- 7.5.5.1.4. Provides independent network connectivity.
- 7.5.5.1.5. Maintains sufficient licensed capacity to recover all critical NHBRC workloads.
- 7.5.5.1.6. Supports encrypted replication between production and DR environments.
- 7.5.5.1.7. Includes orchestration and automation for recovery activities.
- 7.5.5.1.8. Provides recovery support for Active Directory, DNS, SAP and critical business systems.
- 7.5.5.1.9. Includes cyber-recovery capabilities for ransomware and malware events.
- 7.5.5.1.10. Supports controlled failover and failback procedures.
- 7.5.5.1.11. Includes periodic data consistency validation.
- 7.5.5.1.12. Supports annual disaster recovery testing.

7.5.5.2. NHBRC reserves the right to invoke Disaster Recovery during:

- 7.5.5.2.1. Major service outages.
- 7.5.5.2.2. Cybersecurity incidents.
- 7.5.5.2.3. Infrastructure failures.
- 7.5.5.2.4. Natural disasters.
- 7.5.5.2.5. Any event materially impacting service availability.

7.5.6. Migration Alignment

7.5.6.1. The establishment of disaster recovery capabilities shall form part of the migration and transition activities defined in Section 11.

7.5.6.2. The Service Provider shall:

- 7.5.6.2.1. Define the approach for implementing DR during migration
- 7.5.6.2.2. Ensure DR capabilities are tested and validated prior to final production cutover

7.5.7. Testing and Validation

7.5.7.1. The Service Provider shall perform regular testing of backup and disaster recovery capabilities. This includes:

7.5.7.1.1. Annual disaster recovery testing

7.5.7.1.2. Periodic backup restoration testing

7.5.7.2. The Service Provider shall:

7.5.7.2.1. Provide documented test results

7.5.7.2.2. Test results shall be submitted to the NHBRC governance structures for review

7.5.7.2.3. Identify and remediate gaps

7.5.8. Monitoring and Reporting

7.5.8.1. The Service Provider shall monitor backup and DR processes

7.5.8.2. Provide regular reports on:

7.5.8.2.1. Backup success/failure reports

7.5.8.2.2. Recovery readiness status

7.5.8.2.3. Storage capacity and retention

7.5.9. Compliance and Integration

7.5.9.1. The backup and disaster recovery solution shall:

7.5.9.1.1. Align with NHBRC policies and regulatory requirements

7.5.9.1.2. Integrate with hosting, network, and security services

7.5.9.2. The Service Provider shall ensure data remains recoverable throughout the contract lifecycle and supports exit and transition requirements.

7.6. UNIFIED COMMUNICATIONS AND COLLABORATION

7.6.1. The Service Provider shall implement and manage a secure, reliable, and integrated unified communications solution to support NHBRC's communication and collaboration needs.

7.6.2. Collaboration Platform

7.6.2.1. The solution shall align to Microsoft 365 and Microsoft Teams. This includes:

7.6.2.1.1. Configure and manage Microsoft Teams for messaging, meetings, and collaboration

7.6.2.1.2. Ensure integration with Exchange Online, SharePoint Online, and OneDrive

7.6.2.1.3. Support collaboration across the organisation

7.6.3. Voice and Telephony Services

7.6.3.1. The Service Provider shall deliver enterprise voice services integrated with Microsoft Teams.

7.6.3.2. This includes:

7.6.3.2.1. Voice enablement (Direct Routing, Operator Connect, or equivalent)

7.6.3.2.2. Inbound and outbound calling

7.6.3.2.3. Number management and porting

7.6.3.2.4. Call routing, queues, and auto-attendants

7.6.3.3. The bidder shall clearly define the proposed voice architecture and dependencies

7.6.3.4. The solution must ensure high availability and service continuity.

7.6.4. Performance and User Experience

7.6.4.1. The Service Provider shall ensure consistent and high-quality user experience. This includes:

- 7.6.4.1.1. Monitoring of call quality and session performance
- 7.6.4.1.2. Management of latency, jitter, and packet loss
- 7.6.4.1.3. Alignment with network QoS policies (Section 7.3)

7.6.4.2. The Service Provider shall provide reporting on service quality and usage.

7.6.5. Security and Compliance

7.6.5.1. The unified communications solution shall:

- 7.6.5.1.1. Integrate with identity and access management controls
- 7.6.5.1.2. Align with data protection and classification policies
- 7.6.5.1.3. Support secure access for remote and mobile users

7.6.5.2. Security controls must align with Section 7.4 (Security).

7.6.6. Licensing and Optimisation

7.6.6.1. The Service Provider shall:

- 7.6.6.1.1. Manage and optimise Microsoft 365 and voice-related licensing
- 7.6.6.1.2. Ensure efficient allocation of licenses aligned to user needs
- 7.6.6.1.3. Provide recommendations for cost optimisation

7.6.6.2. The Service Provider shall provide regular reporting on:

- 7.6.6.2.1. License utilisation
- 7.6.6.2.2. Usage trends
- 7.6.6.2.3. Optimisation opportunities

7.6.7. Service Management and Support

7.6.7.1. The Service Provider shall:

- 7.6.7.1.1. Provide end-user support for communication services
- 7.6.7.1.2. Manage incidents and service requests
- 7.6.7.1.3. Maintain service availability in line with SLA requirements

7.6.7.2. Minimum SLA schedule

Priority	Acknowledge	Response	Restore
P1 Critical	15 min	30 min	4 hrs
P2 High	30 min	1 hr	8 hrs
P3 Medium	4 hrs	8 hrs	24 hrs
P4 Low	8 hrs	24 hrs	72 hrs

7.6.7.3. Minimum Availability Requirements

Service	Availability
Core Hosting	99.95%
Network Services	99.95%

Internet Services	99.90%
Unified Communications	99.90%
Disaster Recovery Platform	99.90%

7.6.7.4. Service metrics:

- 7.6.7.4.1. Backup success rate $\geq 98\%$.
- 7.6.7.4.2. Critical patch deployment ≤ 14 days.
- 7.6.7.4.3. High-risk vulnerability remediation ≤ 30 days.
- 7.6.7.4.4. Security event notification ≤ 1 hour of detection.
- 7.6.7.4.5. Monthly service reports due within 5 business days.

7.6.8. Integration Requirements

7.6.8.1. The Unified Communications solution must integrate with:

- 7.6.8.1.1. Network and connectivity services (Section 7.3)
- 7.6.8.1.2. Infrastructure Security and monitoring services (Section 7.4)
- 7.6.8.1.3. Identity and access management systems

7.7. SERVICE MANAGEMENT AND GOVERNANCE

7.7.1. The Service Provider shall implement a service management and governance framework to ensure effective delivery, performance management, and continuous improvement of all services

7.7.2. Service Management Processes

7.7.2.1. The Service Provider shall implement and manage core service management processes, including:

- 7.7.2.1.1. Incident, problem, and change management
- 7.7.2.1.2. 24/7/365 service desk support
- 7.7.2.1.3. Incident escalation and resolution management
- 7.7.2.1.4. Monthly, quarterly, and annual service performance reports (including availability, security, and utilisation)
- 7.7.2.1.5. Participation in NHBRC governance structures, including Change Advisory Board (CAB) meetings

7.7.2.2. All processes must:

- 7.7.2.2.1. Be documented and standardised
- 7.7.2.2.2. Align with recognised best practices (e.g. ITIL)
- 7.7.2.2.3. Support audit and compliance requirements

7.7.3. Service Level Management

7.7.3.1. The Service Provider shall deliver services in accordance with agreed Service Level Agreements (SLAs).

7.7.3.2. SLAs shall include measurable targets for:

- 7.7.3.2.1. Service availability
- 7.7.3.2.2. Incident response and resolution
- 7.7.3.2.3. System performance

7.7.3.3. The Service Provider shall:

- 7.7.3.3.1. Monitor SLA performance
- 7.7.3.3.2. Report on SLA compliance
- 7.7.3.3.3. Implement corrective actions where required

7.7.3.4. SLA breaches shall be tracked and reported as part of governance reviews

7.7.4. Service Credits

7.7.4.1. Failure to meet SLA targets shall result in service credits.

7.7.4.2. The Service Provider shall:

- 7.7.4.2.1. Define a clear service credit model
- 7.7.4.2.2. Apply credits consistently for SLA breaches
- 7.7.4.2.3. Implement corrective measures for repeated failures

7.7.5. Service Governance Structure

7.7.5.1. The Service Provider shall participate in structured governance forums, including:

- 7.7.5.1.1. Monthly operational meetings
- 7.7.5.1.2. Quarterly service review meetings
- 7.7.5.1.3. Executive-level governance meetings

7.7.5.2. The Service Provider shall provide:

- 7.7.5.2.1. Service performance reports
- 7.7.5.2.2. SLA compliance reports
- 7.7.5.2.3. Incident and problem summaries
- 7.7.5.2.4. Risk and issue registers

7.7.6. Escalation and Communication

7.7.6.1. The Service Provider shall implement a formal escalation framework.

7.7.6.2. This includes:

- 7.7.6.2.1. Defined escalation levels (operational, management, executive)
- 7.7.6.2.2. Clear communication channels
- 7.7.6.2.3. Timely escalation of critical issues

7.7.7. Continuous Service Improvement

7.7.7.1. The Service Provider shall implement continuous service improvement practices.

7.7.7.2. This includes:

- 7.7.7.2.1. Identification of improvement opportunities
- 7.7.7.2.2. Periodic service reviews
- 7.7.7.2.3. Implementation of agreed improvements

7.7.8. Commercial Benchmarking and Cost Optimisation

7.7.8.1. NHBR reserves the right to conduct benchmarking reviews during the contract period to ensure continued value for money.

7.7.8.2. The Service Provider shall:

- 7.7.8.2.1. Provide required cost and service data

7.7.8.2.2. Participate in benchmarking activities

7.7.9. Service Management Tools

7.7.9.1. The Service Provider shall provide tools to support service delivery.

7.7.9.2. This includes:

7.7.9.2.1. Incident and request management systems

7.7.9.2.2. Monitoring and reporting platforms

7.7.9.2.3. Performance tracking tools

7.7.9.3. The tools must provide visibility to NHBRC and support audit requirements.

7.7.10. Resource Model

7.7.10.1. The Service Provider shall:

7.7.10.1.1. Assign dedicated resources per service component

7.7.10.1.2. Maintain appropriately skilled personnel

7.7.10.1.3. Ensure continuity of key resources

7.7.10.1.4. Align resources with the approved organisational structure

8. TRAINING AND SKILLS TRANSFER

8.1. The Service Provider shall develop and implement a structured skills transfer programme covering all managed services within scope.

8.2. The programme shall include:

- Training of a minimum of three (3) designated NHBRC technical staff
- Coverage of key domains including:
 - Hosting infrastructure
 - Networking and WAN
 - Cybersecurity
 - Cloud services
 - Unified communications
 - Disaster recovery

8.3. Progressive knowledge transfer to enable NHBRC operational self-sufficiency over the contract period

8.4. Practical, hands-on training aligned to live environments

8.5. Workshops and awareness sessions aligned to operational needs

9. DOCUMENTATION

9.1 Documentation Requirements during the contract period

9.2 The Service Provider shall develop and maintain up-to-date documentation for all managed services.

- a) Solution architecture (logical and physical)
- b) Network and system configurations

- c) Operational procedures and runbooks
- d) Security configurations and standards
- e) Roles, responsibilities, and organisational structure
- f) Service management processes

9.3. Documentation Management All documentation shall be:

- 9.3.1.1.1. Be maintained and kept current throughout the contract period
- 9.3.1.1.2. Be updated following changes, upgrades, or material incidents
- 9.3.1.1.3. Be stored in a format accessible to NHBRC

9.4. Documentation shall be provided to NHBRC upon request or during governance reviews

10.

SUPPORT AND ENABLEMENT

10.1 The Service Provider shall provide 24x7x365 technical support across the full ICT environment, including:

- a) Incident management, escalation, and resolution
- b) Infrastructure support across hosting, network, security, cloud, and UC services
- c) Support for upgrades, refreshes, and infrastructure changes

10.2. Assistance with NHBRC ICT projects and initiatives

10.3. Participation in operational and governance forums where required

11.

MIGRATION REQUIREMENTS

11.1. The Service Provider shall plan and execute an end-to-end migration from the current NHBRC environment to the proposed solution.

11.1.1. The migration shall include all service domains:

- 10.3.1.1.1. Migration of existing production systems and services
- 10.3.1.1.2. Implementation of new components required for the target environment, including disaster recovery capabilities

11.2. Migration Approach

11.2.1. The migration shall be executed in structured phases, including:

- a) Assessment and discovery of the current environment
- b) Migration planning and cutover strategy
- c) Pilot migration and validation
- d) Full production migration
- e) Post-migration stabilisation and support

11.2.2. The migration timeline shall be proposed by the bidder and approved by NHBRC.

11.3. Migration Requirements

11.3.1. The Service Provider shall provide:

- 11.3.1.1.1. Incumbent provider handover.
- 11.3.1.1.2. Environment discovery and assessment.
- 11.3.1.1.3. Application dependency mapping.
- 11.3.1.1.4. Licensing transfer activities.
- 11.3.1.1.5. Security and penetration testing.
- 11.3.1.1.6. Data validation and reconciliation.
- 11.3.1.1.7. Number porting for telephony services.
- 11.3.1.1.8. Pilot migration activities.
- 11.3.1.1.9. Parallel-run period where applicable.
- 11.3.1.1.10. Change freeze management.
- 11.3.1.1.11. Rollback procedures.
- 11.3.1.1.12. Business continuity arrangements.
- 11.3.1.1.13. Hypercare support following go-live.
- 11.3.1.1.14. Legacy environment decommissioning.

11.3.2. Acceptance Criteria

11.3.3. Migration shall only be deemed complete after:

- 11.3.3.1.1. Successful testing.
- 11.3.3.1.2. User acceptance.
- 11.3.3.1.3. Documentation handover.
- 11.3.3.1.4. Knowledge transfer completion.
- 11.3.3.1.5. Formal NHBRC sign-off.

11.4. Transition Requirements

11.4.1. The Service Provider shall ensure:

- a) Minimal downtime during migration activities
- b) Controlled and approved cutover processes
- c) Implementation of rollback strategies for critical systems
- d) Validation of services prior to final cutover
- e) No disruption to critical business services during business hours, unless approved by NHBRC

11.5. Testing and Acceptance

11.5.1. The Service Provider shall:

- a) Perform pre-cutover testing of all services
- b) Validate performance, security, and connectivity in the new environment
- c) Obtain NHBRC sign-off prior to final production cutover

11.6. Handover and Close-Out

11.6.1. Upon completion of migration, the Service Provider shall:

- a) Provide as-built documentation of the migrated environment
- b) Deliver updated architecture, configuration, and operational documentation

- c) Conduct formal handover to NHBRC ICT teams
- d) Complete knowledge transfer activities and obtain sign-off

12. DELIVERABLES

- 12.1. The Service Provider shall deliver the following:
 - 12.1.1. A detailed implementation plan including phases, milestones, dependencies, resources, and timelines for all managed services.
- 12.2. Implementation and Migration
 - 12.2.1. Detailed implementation plan (phases, milestones, dependencies, timelines)
 - 12.2.2. Migration and transition plan including:
 - a) Hosting infrastructure
 - b) Network and connectivity
 - c) Unified communications
 - d) Disaster recovery implementation
 - e) Rollback and recovery strategy
- 12.3. Solution Design Documentation
 - a) Logical and physical architecture
 - b) Security architecture
 - c) Integration architecture across all services
 - d) Network and connectivity diagrams
- 12.4. Backup and Disaster Recovery
 - 12.4.1. Disaster recovery plan, including architecture and procedures
 - 12.4.2. DR test reports and remediation actions
 - 12.4.3. Backup strategy, including:
 - a) Policies and schedules
 - b) Retention rules
 - c) Restoration procedures
 - d) Evidence of restore testing
- 12.5. Service Reporting
 - 12.5.1. Monthly reports including:
 - a) SLA performance and availability
 - b) Capacity and utilisation
 - c) Security posture summary
 - d) Incident and root cause analysis
- 12.6. Knowledge Transfer
 - 12.6.1. Skills transfer plan
 - 12.6.2. Training materials and documentation

12.6.3. Operational runbooks and procedures

12.6.4. Formal handover to NHBRC

12.7. Exit and Transition Management

12.7.1. The Service Provider shall develop and maintain a detailed Exit Management Plan.

12.7.2. The plan shall include:

- 12.7.2.1. Data handover procedures.
- 12.7.2.2. Configuration exports.
- 12.7.2.3. Administrative credential transfer.
- 12.7.2.4. Asset transfer requirements.
- 12.7.2.5. Licensing transfer arrangements.
- 12.7.2.6. Knowledge transfer activities.
- 12.7.2.7. Documentation handover.
- 12.7.2.8. Successor-provider support.
- 12.7.2.9. Service transition staffing.
- 12.7.2.10. Secure destruction procedures.
- 12.7.2.11. Decommissioning activities.

12.7.3. No vendor lock-in mechanisms shall be permitted.

12.8. Exit and Transition Support

12.8.1. The Service Provider shall provide exit support upon contract expiry or termination.

12.8.2. The exit period shall:

- a) Be a minimum of three (3) months and up to six (6) months
- b) Form part of the contract terms

12.8.3. During this period, the Service Provider shall:

- a) Ensure uninterrupted service delivery
- b) Provide full cooperation with NHBRC and any successor provider
- c) Transfer all services and operational responsibilities

12.8.4. The Service Provider shall provide:

- a) Complete and up-to-date documentation
- b) Administrative access and system credentials
- c) Knowledge transfer sessions

12.8.5. The Service Provider shall:

- a) Continue to meet SLA requirements
- b) Not degrade service levels

12.8.6. No additional exit fees shall be charged, except where pre-approved by NHBRC.

12.8.7. Failure to comply shall constitute a material breach of contract.

12.9. Exit Management Deliverables

12.9.1. The Service Provider shall:

- 12.9.1.1.1. Deliver the initial Exit Management Plan within 30 calendar days of contract commencement.
- 12.9.1.1.2. Review and update the Exit Plan annually.
- 12.9.1.1.3. Conduct an executable exit readiness test during the final year of the contract.
- 12.9.1.1.4. Maintain ownership records for all assets, documentation, automation scripts, credentials, and configurations.
- 12.9.1.1.5. Provide secure deletion certificates upon completion of transition.

13. DURATION

- 13.1. The contract shall include:
 - 13.1.1.1.1. Annual performance reviews.
 - 13.1.1.1.2. Annual value-for-money reviews.
 - 13.1.1.1.3. Benchmarking reviews.
 - 13.1.1.1.4. Audit rights.
 - 13.1.1.1.5. Change-control governance processes.
 - 13.1.1.1.6. Termination for material breach.
 - 13.1.1.1.7. Termination for repeated SLA failures.
 - 13.1.1.1.8. Termination for insolvency.
 - 13.1.1.1.9. Termination for serious security breaches.
 - 13.1.1.1.10. Termination for convenience subject to contractual notice periods.
- 13.2. The five-year term shall commence upon signing of contract.
- 13.3. The contract shall include an initial implementation and migration phase, during which the Service Provider shall achieve service stability and operational readiness prior to full-service commencement, as defined in Section 11 (Migration Requirements).
- 13.4. Any extension or renewal of the contract shall be subject to:
 - a) NHBRC approval
 - b) Performance against agreed SLAs
 - 13.4.1.1.1. Budget availability and procurement governance requirements
- 13.5. Upon expiry or termination of the contract, the Service Provider shall comply with the exit and transition requirements defined in Section 12 (Deliverables).
- 13.6. The contract shall be governed by provisions relating to:
 - a) Asset ownership
 - b) Exit and transition obligations
 - c) Commercial benchmarking
- 13.7. These provisions shall remain binding for the full duration of the contract, including any extensions.

14. SERVICE EXPECTATION

- 14.1. The NHBRC standard working hours are 08:30 to 16:30, Monday to Friday. The Service Provider shall ensure resource availability and service coverage within these hours.
- 14.2. The Service Provider shall ensure resources are available for support, escalation, and operational requirements as reasonably required by NHBRC, including after-hours support for critical incidents.
- 14.3. The Service Provider shall deploy suitably skilled resources either:
 - 14.3.1. On-site at NHBRC premises, or
 - 14.3.2. Remotely in accordance with NHBRC policies and operational requirements.
- 14.4. Resource deployment shall ensure continuity of services and achievement of agreed SLAs.
- 14.5. The Service Provider shall ensure that all service delivery models, including asset ownership structures and transition arrangements, support long-term operational sustainability and avoid vendor lock-in.
- 14.6. The Service Provider shall execute all assigned tasks and deliverables within agreed timeframes and in accordance with approved service management processes.
- 14.7. The Service Provider shall propose and implement cost-effective service delivery models that optimise performance, efficiency, and value for money, while meeting NHBRC operational requirements.
- 14.8. All queries, requests, and operational communications from NHBRC shall be acknowledged as per the priority matrix, with resolution timelines governed by the applicable SLA classification.

15. REPORTING

- 15.1. The Service Provider shall implement end-to-end monitoring across all managed services, including hosting, network, WAN, internet, unified communications, and disaster recovery environments to ensure continuous visibility of availability, performance, security, and data integrity.
- 15.2. The Service Provider shall provide monthly service reports covering, at a minimum:
 - 15.2.1. SLA performance and compliance
 - 15.2.2. System uptime and availability
 - 15.2.3. Capacity and utilisation trends
 - 15.2.4. Security incidents and posture summary
 - 15.2.5. All incidents, outages, and service interruptions
- 15.3. The Service Provider shall maintain real-time monitoring, alerting, and incident logging capabilities to enable proactive detection, escalation, and resolution of service issues.
- 15.4. At contract termination or expiry, the Service Provider shall submit a comprehensive end-of-contract report detailing:
 - 15.4.1. Overall service performance against SLAs

- 15.4.2. Major incidents and recurring risks
- 15.4.3. Capacity and infrastructure utilisation trends
- 15.4.4. Security posture and key vulnerabilities
- 15.4.5. Recommendations for service optimisation and continuous improvement

16. REPORTING

16.1. GENERAL REQUIREMENTS

- 16.1.1. The NHBRC requires submissions from competent and experienced organisations with proven capability in Managed Hosting Infrastructure Services, Unified Communications, and Business Continuity and Disaster Recovery.
- 16.1.2. Bidders shall provide verifiable evidence of relevant experience and technical capability.

16.2. REQUISITES OF THE SERVICE PROVIDER

- 16.2.1. Bidders must submit a comprehensive proposal including the following:
- 16.2.2. A clear articulation of the bidder's understanding of the Terms of Reference and scope of services.
- 16.2.3. **Details of the proposed project team, including:**
 - a) Roles and responsibilities
 - b) CVs of key personnel
 - c) Certified copies of qualifications (not older than 6 months)
 - d) Relevant certifications and experience
- 16.2.4. **Description of the bidder's quality assurance methodology, including:**
 - a) Service delivery controls
 - b) Governance processes
 - c) Risk and issue management approach
- 16.2.5. **A detailed Pricing Schedule must be submitted in accordance with Annexure C to Annexure H.**

16.3. SUMMARY OF PROJECTS EXECUTED AND COMPLETED

- 16.3.1. The bidder must demonstrate proven experience in delivering similar projects within the last five (5) years.

16.3.2. The following information must be submitted:

Name of Project	Project Description	Contract Value (incl. VAT)	Contract Duration	Client Name	Client Contact Tel

16.3.3. Each listed project above must be supported by:

16.3.3.1.1. Signed client reference letter on official letterhead

16.3.3.1.2. Confirmation of successful project completion

16.3.3.1.3. Contactable client reference

16.3.3.1.4. Project value

16.4. KEY PERSONNEL REQUIREMENTS

16.4.1. Bidders must assign suitably qualified and experienced personnel to the project.

16.4.2. A summary of key personnel must be provided in the following format:

No.	Full Name	Role	Qualifications	Specialisation	Years of Experience
1.					
2.					
3.					
4.					
5.					

***Please attach recently (last 6 months) certified copies of academic qualifications.**

Note: in addition, please provide the following:

16.4.3. CV for each of the project team members highlighting specific and relevant qualifications and experience.

16.4.4. Key personnel may only be replaced by personnel with similar expertise over the life of the contract and written permission must be obtained from the NHBRC.

16.4.5. Provide project details of projects that were successfully completed in the last five (5) years in the format above. For each of these projects, a reference letter of successful completion of the project must be provided by the **client, on the client's letterhead, and signed off by an authorised** delegated employee of the client.

REFERENCE LETTER FORMAT

Name of project:

Name of Client:

Client Contact Details

Contact person:

Role in Project:

Contact Tel No:

Contact Cell:

Project Start Date:

Project Completion Date:

Contract Amount (incl. VAT):

Summary of Project (maximum 200 words).

17. PROJECT PROPOSAL

- 17.1. The bidder is required to submit a comprehensive project proposal outlining its approach to delivering the required managed services.
- 17.2. The bidder shall clearly describe its proposed approach and methodology for executing the project, including how the solution addresses all requirements defined in the Scope of Work.
- 17.3. The methodology must cover:
- a) Service delivery approach
 - b) Resource deployment model
 - c) Governance and reporting approach
 - d) Risk management approach
 - e) Service transition and operational readiness
- 17.4. The bidder must submit a detailed project implementation plan, including:
- a) Project phases and milestones
 - b) Key activities and dependencies
 - c) Timelines aligned to deliverables
 - d) Resource allocation plan
- 17.5. The project plan must demonstrate a structured approach to implementation and service readiness.
- 17.6. The bidder must provide a detailed migration plan covering:
- a) End-to-end transition methodology
 - b) Process flow and sequencing of migration activities
 - c) Cutover strategy and validation approach
 - d) Rollback and contingency planning
 - e) Timeline linked to key migration deliverables

- 17.7. The implementation period is expected to be approximately a minimum of three (3) months and maximum six months; however, alternative timeframes may be proposed, subject to NHBRC approval and operational continuity requirements.

18. SITE ASSESSMENT (NON-MANDATORY RECOMMENDATION)

- 18.1. Bidders are encouraged, but not required, to conduct site assessments of the NHBRC offices and facilities to inform the development of their proposals.
- 18.2. Such assessments are intended to:
- a) Provide a better understanding of existing infrastructure and environmental conditions
 - b) Support accurate solution design and pricing
 - c) Reduce assumptions and associated implementation risks
- 18.3. Bidders shall ensure that any site visits or assessments are coordinated with the NHBRC and conducted in accordance with applicable access and security requirements.

19. PROPOSED TECHNOLOGY STACK SCHEDULE

- 19.1. Bidders shall submit a detailed Technology Stack Schedule covering all technologies, platforms, and service components proposed as part of the solution.
- 19.2. The schedule will be used by NHBRC to:
- a) Evaluate technical suitability
 - b) Validate OEM alignment and accreditation
 - c) Assess interoperability and supportability
 - d) Confirm alignment between the proposed solution, architecture, and pricing
- 19.3. Failure to submit a complete Technology Stack Schedule may result in the bidder being deemed non-compliant.
- 19.4. The bidder shall clearly identify all third-party, hosted, subcontracted, or OEM-delivered services forming part of the solution.
- 19.5. Bidders shall ensure that all technologies listed are supported for the duration of the contract and are aligned to vendor lifecycle and support policies.
- 19.6. Bidders shall complete the following schedule:

SERVICE DOMAIN	TECHNOLOGY / PRODUCT	OEM / VENDOR	HOSTING MODEL (ON-PREM / CLOUD / HYBRID)	LICENSING MODEL	OEM ACCREDITATION	SUPPORT MODEL
HOSTING INFRASTRUCTURE						
VIRTUALISATION PLATFORM						
BACKUP & DR						

WAN / SD-WAN						
NETWORK SWITCHING						
FIREWALL / SECURITY						
ENDPOINT SECURITY (EDR)						
UNIFIED COMMUNICATIONS						
MONITORING & MANAGEMENT						
CLOUD SERVICES						

20. PROPOSED TECHNOLOGY STACK SCHEDULE

20. EVALUATION STAGES

20.1.1. In accordance with NHBRC Supply Chain Management Policy, bids will be evaluated in three (3) stages:

- **Stage 1:** Mandatory Compliance
- **Stage 2:** Functional Evaluation
- **Stage 3:** Price and Preference Points Evaluation

20.1.2. Only bidders who are fully compliant with Stage 1 and achieve the minimum functionality threshold in Stage 2 will be considered for Stage 3.

20.2. Stage 1: Compliance check of Bid Requirements

Mandatory documents for disqualification as per the Checklist in this RFP should be completed in full, signed and submitted with the Bidder's response to this RFP. Failure to comply with the "mandatory documents will result in the disqualification of the Bidder.

Submission of false, fraudulent, or misleading information or documents will result in the disqualification of the Bidder or termination of the successful bidder's contract. In this regard, the NHBRC reserves its rights to take appropriate legal action.

LEGISLATIVE DOCUMENTS TO BE SUBMITTED NOT FOR DISQUALIFICATION

No.	Bidders shall take note of the following bid conditions / Legislative Submissions.	Yes/No
1	SBD 3.1 Pricing Schedule (Firm Price) Make sure it is completed	
2	SBD 6.1 The Preference claim form should be completed and signed, regardless if points are claimed or not.	
3	SBD 7.2 (Contract Form, should be completed and signed)	
4	Bidder should submit CSD (Central Supplier Database) Report/ MAAA Number	
5.	Latest CIPC Documents	
6.	Valid SARS-issued PIN Code	

7.	Signed teaming agreement	
8.	Certified Identification documentation of company directors	

MANDATORY DOCUMENTS TO BE SUBMITTED FOR DISQUALIFICATION		
No.	Bidders shall take note of the following bid conditions / Mandatory Submissions.	Yes/No
1.	SBD 4 (Bidders Disclosure Form, Make sure it is completed and signed)	
2.	Annexure C TO H Pricing schedule: including a detailed costing breakdown of all costs. The pricing schedule (Annexure H) must be duly signed by the bidder/ and or a duly authorized individual by way of resolution which must be attached to the bid, if there is no signature on the pricing schedule the bidder will be disqualified (Mandatory)	
3.	Audited Financial Statements or reviewed financial statements by independent reviewers for close corporations for the last three (03) financial years, will be used to determine the bidder's financial soundness. (Mandatory)	
4.	<u>ISO / IEC 27001(Mandatory)</u> <i>The bidder must hold a valid ISO/IEC 27001 certification issued to the organisation by an accredited certification body.</i> Requirements: • Certification must be current and valid at the time of submission • Certification scope must be relevant to the services proposed • The certification must be maintained before and after appointment by NHBRC NHBRC reserves the right to verify certification validity and scope.	
5.	<u>OEM / Vendor Partnerships (Mandatory)</u> Bidders must provide proof of active OEM accreditation or partnership relevant to the proposed solution. This includes (where applicable): • Hosting infrastructure • Networking and WAN services • Internet access services • Unified communications • Backup and disaster recovery • Cloud and virtualisation platforms Bidder shall submit: • Valid OEM partnership agreements /MOU, certificates, or authorisation letters • Details of any third-party partners or subcontractors Where third parties are used: • The bidder must provide formal agreements • The bidder remains fully responsible for service delivery NHBRC reserves the right to verify all submitted OEM partnerships.	
6.	<u>REGULATORY COMPLIANCE - ICASA or ISPA (Mandatory)</u> Bidders must demonstrate compliance with all telecommunication's regulatory requirements in South Africa. Bidders shall provide one or more of the following (where applicable): • ICASA licence (ECS/ECNS or equivalent) • ISPA membership	

	- Agreement with a licensed third-party provider (e.g., SLA, contract, MOU, or letter of authorisation). Where third-party providers are used: - Details of the provider must be submitted - Proof of licensing must be provided - The bidder's role must be clearly defined All equipment must be ICASA type approved. <i>The bidder remains fully responsible for regulatory compliance.</i>	
7.	<u>Data Centre Certification (Mandatory)</u> Bidders must provide valid certification for the proposed primary hosting facility. ensuring it meets recognised standards for availability, redundancy, and resilience. Minimum Requirements: - Uptime Institute Tier III OR - TIA-942 Rated 3 The bidder must submit: - Certification evidence - Validity period NHBRC reserves the right to verify the authenticity and validity of all submitted certifications with the issuing authority Failure to provide valid certification will result in disqualification.	
8.	<u>Hosting and Disaster Recovery (DR) site</u> Bidders must demonstrate legal access to the proposed primary and disaster recovery facilities located within South Africa. The bidder shall submit: - Proof of ownership, lease, co-location, or cloud hosting agreements All agreements must: - Be valid and signed - Reflect the bidder's legal entity - Cover the contract duration or include renewal provisions Where third-party facilities are used, bidders must provide: - Facility location - Hosting provider details - Nature of the hosting arrangement Acceptable proof may include: - Proof of facility ownership - Valid lease agreements - Co-location agreements - Cloud hosting agreements - Memoranda of Understanding (MOU) - Legally binding service or hosting agreements with the facility owner or hosting provider All submitted proof must: - Clearly reflect the bidder's legal entity name - Clearly indicate the duration of the agreement, which must cover or exceed the contract period (or include renewal/extension provisions)	

	• Be signed by duly authorised representatives of both parties • Be dated and valid at the time of bid submission • Clearly confirm the bidder's right to utilise the facility for hosting and/or DR services The NHBRC reserves the right to verify all submitted information and agreements and may conduct site inspections of proposed facilities or request a demo of proposed Hosting and DR site. Notwithstanding the use of third-party facilities, the bidder shall remain fully responsible for the availability, performance, security, and compliance of the proposed hosting and disaster recovery solution. Failure to provide verifiable, signed, and valid proof of facility access and hosting rights will result in the bidder being deemed non-responsive.	
--	--	--

Note: NHBRC will be using General Conditions of Contract (GCC) as issued by the National Treasury and SLA for the management of the contract

20.3. Stage 2: Functionality in terms of the set technical evaluation criteria

- 20.3.1. Bids must fully comply with all the Mandatory Requirements for **Stage 1: Compliance check of Mandatory Requirements** to qualify for **Stage 2: Functional Evaluation** and those bids which failed to comply with all the requirements of **Stage 1** will be invalidated or disqualified from the process.

The Bidders information will be scored according to the following points systems:

The following values and formulae will be applicable when evaluating the bid

Member score for criteria

X Weight per criteria = Total Score per criteria

Highest points for criteria

5= Excellent 4= Very good 3= Good 2= Average 1= Poor 0= Non-compliance

20.4. STAGE 2: FUNCTIONAL EVALUATION

Item No.	Evaluation Criteria	Description	Weight (%)
1	Bidder Capability	The bidder must demonstrate experience in delivering managed infrastructure solutions of similar scope and complexity. Submission Requirements: • Minimum of three (3) projects • Appointment letter per project (3) • Matching reference letter per project (3) (as per Section 16.4.5) Scoring Allocation: No valid submissions = 0 1 valid Appointment Letter + Matching valid Reference Letter = 1 2 valid Appointment Letters + 2 Matching valid Reference Letters = 2 3 valid Appointment Letters + 3 Matching valid Reference Letters = 3 4 valid Appointment Letters + 4 Matching valid Reference Letters = 4 >=5 valid Appointment Letters + >=5 Matching valid Reference Letters = 5	40
2	Project Manager's Capability	The bidder must propose a qualified Project Manager with relevant experience. Submission Requirements: • CV detailing experience and roles • Minimum 5 years relevant experience • Certified qualifications NQF 7 level 1) Information Technology, Computer Science, Information Systems, or a related field; OR 2) Project Management or Management-related qualification, supported by demonstrable experience in ICT infrastructure projects. • Project management certification (PMP, PRINCE2, Agile or related) • Evidence of similar projects (minimum 2) • Reference letters confirming role (as per Section 16.4.5) Scoring Allocation: 0 = No CV submitted OR no verifiable evidence 1 = CV submitted with less than 5 years' relevant experience OR missing	10

Item No.	Evaluation Criteria	Description	Weight (%)
		qualification/certification 2 = CV demonstrating minimum 5 years' relevant experience + qualification + certification 3 = CV with minimum 5 years' experience + qualification + certification + 1 verifiable reference letter 4 = CV with minimum 5 years' experience + qualification + certification + 2 verifiable references letters 5 = CV with minimum 5 years' experience + qualification + certification + 3 or more verifiable references letters.	
3	Project Team's Capability	The bidder must submit CVs for three (3) key technical resources plus a Service Manager (at least four proposed resources). Each resource must include: • A detailed Curriculum Vitae (CV) • A relevant qualification (minimum NQF Level 6 or higher in Information Technology or related field) • At least one relevant industry certification aligned to the proposed solution (e.g. networking, cloud, virtualisation, cybersecurity, or infrastructure management) • A minimum of three (3) years' relevant experience in managed infrastructure environments Scoring Allocation: 0 = No CV OR qualification submitted 1 = CV submitted with less than 3 years' relevant experience OR missing qualification/certification 2 = CV with 3 years' relevant experience + qualification + 1 certificate 3 = CV with 3 years' experience + qualification + 1 certificate 4 = CV with 4 years' experience + qualification + 1 certificate 5 = CV with mor than 5 years' experience + qualification + 2 or more certificates	20
4	Migration Plan	The bidder must submit a migration and transition plan. The plan must include: • Migration approach and methodology • Timeline (e.g. Gantt chart) less than or equal 6months and defined phases • Deliverables and phases • Risk and mitigation plan • Cutover approach Scoring Allocation 0 = No migration plan submitted 1 = Migration plan submitted but includes only 1–2 of the following: 3 = Migration plan includes at least 3–4 of the following: 5 = Migration plan includes ALL of the following:	10

Item No.	Evaluation Criteria	Description	Weight (%)
		- Migration approach and methodology - Timeline (e.g. Gantt chart) less than or equal 6months and defined phases - Deliverables and milestones - Risk and mitigation plan - Cutover approach	
5	Technical Solution & Architecture	The bidder must submit a comprehensive technical solution. This must include: • Logical and physical architecture • Integration across all service components • High availability and scalability design • DR and failover capabilities • Technology stack description Scoring Allocation: 0 = No submission OR no relevant solution provided 1 = Submission includes only 1–2 of the required components 3 = Submission includes 3–4 of the required components 5 = Submission includes all required components: - Logical and physical architecture - Integration across all service components - High availability and scalability design - Disaster recovery and failover capabilities - Technology stack description	20
TOTAL			100 Points
MINIMUM QUALIFYING REQUIREMENT			70 Points

NB: Only bidders who score 70 points or more out of 100 points will qualify for Stage 3.

The minimum threshold for functionality is 70 out of 100 points. Bidders who fail to meet the minimum threshold will be disqualified and will not be evaluated further for price and preference points.

20.5. STAGE 3: PRICE AND PREFERENCE POINTS EVALUATION

20.5.1. Only bids that have obtained a minimum qualifying score of 70 points in Stage 2 (Functional Requirements) will be evaluated further.

20.5.2. The contract will be awarded in terms of Regulation 4 of the Preferential Procurement Regulations pertaining to the Preferential Procurement Policy Framework Act, 2000 (Act 5 of 2000) and the Preferential Procurement Regulations, 2022. Bids will be adjudicated in terms of the 90/10 preference points system.

90/10 preference point system for acquisition of goods or services with Rand value above R50 million

The following formula must be used to calculate the points out of 90 for price in respect of a tender with a Rand value above R50 million, inclusive of all applicable taxes:

$$P_s = 90 \left(1 - \frac{P_t - P_{min}}{P_{min}} \right)$$

Where:

- P_s = Points scored for price by the bid under consideration
- P_t = Comparative price of the bid under consideration
- P_{min} = Comparative price of the lowest acceptable bid

$$P_s = 90 \left(1 - \frac{P_t - P_{min}}{P_{min}} \right)$$

20.5.3. The points scored will be rounded off to the nearest two decimal places. Points will be awarded to a bidder in accordance with the table below:

20.5.4. A maximum of 10 points may be awarded to a bidder for Preference Points specified in the tender.

Preference Points	Points Allocated
Women	6
Youth	3
Disabilities	1
Military Veterans	0
TOTAL	10 Points

The formula should be written clearly as:

$$NEP = NOP \times \frac{EP}{100}$$

Where:

- *NEP*= Points awarded for equity ownership Preference Points
- *NOP*= The maximum number of points awarded for Preference Points
- *EP*= The percentage of equity ownership (%)

$$NEP = NOP \times \frac{EP}{100}$$

The points scored for price will be added to the points scored for preference points to obtain the Bidder's total points scored out of 100 points.

21. AVAILABILITY OF THE RFP DOCUMENT

- 21.1. Bid documents can be downloaded on the NHBRC Website (www.nhbrc.org.za/current-tenders) and National Treasury eTender Portal (<https://www.etenders.gov.za/>) from **04 September 2026**.
- 21.2. There will be a non-compulsory virtual briefing session that will be held on **11 September 2026 at 11h00**
- 21.3. Link for virtual non-compulsory briefing session:
<https://teams.microsoft.com/meet/362252380611593?p=A3aKrMazq1s4rr5C4p>
- 21.3.1. The link can also be accessed on the NHBRC website

22. RFP CLOSING DATE

- 22.1. RFP Proposal should be marked for Attention: Supply Chain Manager and submitted online via National Treasury eTender Portal (<https://www.etenders.gov.za/>) as per closing.
- 22.2. **No physical or emailed RFP proposals will be accepted.**
- 22.3. **No late submissions will be accepted.**

23. VALIDITY PERIOD OF BIDS

- 23.1. All bids submitted by the bidders must be valid for a period of 90 days from the closing date specified above.

24. ENQUIRIES DIRECTED TO

- 24.1. The administrative enquiries may be directed to:
Department: Supply Chain Management
Contact Person: Mr Kabelo Phalane
E-mail address: Kabelo@nhbrcsa.onmicrosoft.com
- 24.2. Clarifications and enquiries should be sent to Kabelo@nhbrcsa.onmicrosoft.com, tenders@nhbrc.org.za up to 25 September 2026. Responses will be communicated during weekdays, between Monday and Friday from 8:30 am to 16:30 pm.
- 24.3. Responses will be communicated during weekdays, between Monday and Friday from 8:30 am to 16:30 pm.

25. SUBMISSION OF PROPOSALS

25.1. ONLINE BID SUBMISSION

- 25.1.1. Bidders must submit their bids online in a PDF format through the e-Tender Publication portal.
- 25.1.2. The online e-Tender publication portal can be accessed at the following link:
<https://www.etenders.gov.za/>
- 25.1.3. The guide for online bid submission is attached. <https://youtu.be/B7pNseNJYHM>
- 25.1.4. Bidders are to adhere to all the rules for the online bid submission, as the submission must contain the returnable SCM documentation and relevant supporting documents and must contain a signed pricing schedule.
- 25.1.5. For identification purposes bidders are requested to ensure that proposals contain the company's details and are easily identifiable by company logo or name.
- 25.1.6. Non-compliance with online bid submission WILL invalidate the bidder's response.
- 25.1.7. Bidders must take note of and carefully comply with the submission requirements outlined under Stage 1, Stage 2, Stage 3 and ensure all required documents are submitted accordingly.

26. DISCLAIMER

26.1. DUE DILIGENCE

- 26.1.1. The State reserves the right to:
- 26.1.2. Conduct due diligence during the evaluation process to determine the ability of the bidder to honour contractual obligations that might emanate from this tendering process. The due diligence is not only limited to the bidder but to all parties the bidder might have confirmed to do business with for the fulfilment of the contract that might be awarded.
 - 26.1.2.1. Conduct due diligence prior to final award or at any time during the contract period, and this may include pre-announced/ non-announced site visits. During the due diligence process, the information submitted by the bidder will be verified, and any misrepresentation thereof may disqualify the bid in whole or in part.
 - 26.1.2.2. Conduct any evaluation verifications prior to final award or at any time during the contract term period.

26.2. NEGOTIATIONS

- 26.2.1. The State reserves the right to negotiate with the shortlisted bidders prior to or post-award. The terms and conditions for negotiations will be communicated to the shortlisted bidders prior to the invitation to negotiations. This phase is meant to ensure value for money is achieved through the measure of quality that will assess the monetary cost of the goods or services against the quality and or benefits of that goods or services.

26.3. RIGHT OF AWARD

- 26.3.1. The State reserves the following rights –
- 26.3.2. Not to make any award in this bid or accept any bids submitted,
- 26.3.3. Appoint one service provider
- 26.3.4. Request further technical information from any bidder after the closing date,
- 26.3.5. Verify information and documentation of the bidder(s),
- 26.3.6. To withdraw or amend any of the bid conditions by notice in writing to all bidders prior to closing of the bid and post-award.

26.3.7. If an incorrect award has been made, to remedy the matter in any lawful manner it may deem fit.

26.4. APPOINTMENT OF BIDDERS

26.4.1. On approval of the recommendation/s and appointment/s, the successful bidder will sign an acceptance letter together with the Service Level Agreement (SLA). All official instructions, delegated authorities, and reporting lines will be strictly governed by the SLA to be signed by the NHBRC and the successful bidder.

Once the successful bidder has been appointed/awarded, they cannot do any cession to waive or cede without consultation with the NHBRC.

26.5. FRONTING

26.5.1. The NHBRC supports the spirit of broad-based black economic empowerment and recognizes that real empowerment can only be achieved through individuals and businesses conducting themselves in accordance with the Constitution and in an honest, fair, and equitable.

26.5.2. The NHBRC, in ensuring that bidders conduct themselves in an honest manner, will, as part of the bid evaluation processes, conduct or initiate the necessary enquiries/investigations to determine the accuracy of the representation made in this bid document. Should any of the fronting indicators as contained in the Guidelines on Complex Structures and Transactions and Fronting, issued by the Department of Trade, Industry and Competition, be established during such enquiry/investigation, the onus will be on the bidder to prove that fronting does not exist.

26.5.3. Failure to do so by the bidder within a period of fourteen (14) days from the date of notification by NHBRC may invalidate the bid/contract and may also result in the restriction of the bidder to conduct business with the public sector for a period not exceeding ten (10) years, in addition to any other remedies the NHBRC may have against the bidder concerned.

26.6. RESPONSIVE BIDS

26.6.1. Bidders are required to submit responsive bids by ensuring compliance to documents listed under 7.3.1. Non-submission of complete documents as stated will invalidate the bid (**Annexure H**).

26.7. TERMS AND CONDITIONS

26.7.1. NHBRC reserves the right to change or supplement any information or to issue any addendum to this bid before the closing date and time. The NHBRC and its officers, employees and advisers will not be liable in connection with either the exercise of, or failure to exercise this right.

26.7.2. If NHBRC exercised its right to change or supplement information in terms of the above, it may seek an amended bid document from all bidders.

- 27.1. The NHBRC is committed to adhering to the Protection of Personal Information Act 4 of 2013 and the Promotion of Access to Information Act 2 of 2000. To this end, the NHBRC has published its Information Manual on its website, which regulates how NHBRC processes information.
- 27.1.1. The NHBRC requires the information requested in bids for the purpose set out in paragraph 2.5 of the Manual. Further, the Manual confirms that NHBRC processes the information requested in bids from prospective service providers and third parties in paragraph 3.4.
- 27.1.2. Bidders should note that the NHBRC is committed to securing all the information submitted from bidders, in terms of paragraph 6 of the Manual. (included on the NHBRC website)
- 27.1.3. Bidders are in turn required to comply with the tender requirements and when the information of third parties is required by NHBRC, bidders are by law required to obtain the consent of such third parties for the sharing of such third parties' information with the NHBRC.

ANNEXURE A SAP LANDSCAPE

PRODUCTION SAP LANDSCAPE AND SERVER SPECIFICATIONS

Detail	Disk Space (GB)	Memory (GB)	Processor (GHz)
SAP Solution Manager	2350	64	8
SAP Governance, Risk and Compliance 10	2400	32	4
SAP Customer Relationship Management (Central Instance)	4000	80	8
SAP Enterprise Resource Planning (Central Instance)	8000	80	8
SAP Portal	1100	80	8
SAP Business Objects	1000	64	8
SAP Business Warehouse	3000	64	8
SAP Process Integration/Orchestration	1500	64	8
SAP Mobility	1500	80	8
SAP Web Dispatcher (Installed in DMZ)	500	16	4
System Landscape Directory	1000	24	4
TREX	600	32	4
Open Text Archive Server	4100	32	4
Open Text Content Server Back-End Server	1000	16	6
Open Text Content Server Front-End Server	1000	16	6
Open Text Web Server	500	8	4

Open Text SEA Server	320	8	2
----------------------	-----	---	---



B1. NHBRC'S CURRENT BASELINE

Bidders must propose solutions that meet or exceed these requirements and clearly indicate any proposed enhancements.

B2. SITE CONNECTIVITY REQUIREMENTS

Bidders must maintain or improve the resilience model per site and may propose alternative technologies where justified

#	Provincial Office	Primary Connectivity	Secondary Connectivity
1	Cape Town	Fiber	Microwave
2	Durban	Fiber	Microwave
3	Bloemfontein	Fiber	Microwave
4	Rustenburg	Fiber	Microwave
5	Nelspruit	Fiber	Microwave
6	Port Elizabeth	Fiber	Microwave
7	Pretoria Hatfield	Fiber	Microwave
8	Polokwane	Fiber	Microwave
9	Sunninghill	Dual Fiber	Microwave
10	Eric Molobi Soshanguve	Fibre	Microwave
11	George	Fiber	LTE
12	Newcastle	Fiber	LTE
13	Richards Bay	Fiber	LTE
14	Bethlehem	Fiber	LTE
15	Klerksdorp	Fiber	LTE
16	Mahikeng	Fiber	LTE
17	Witbank	Fiber	LTE
18	East London	Fiber	LTE
19	Tzaneen	Fiber	LTE
20	Modimolle	Fiber	LTE
21	Thohoyandou	LTE	LTE
22	Kimberly	Fiber	LTE

B3. DISTRIBUTION SWITCHING REQUIREMENTS

Core & Distribution Infrastructure

Component	Quantity	Throughput
Distribution Switches	35	Minimum switching capacity of 688 Gbps per switch or equivalent vendor-recommended architecture providing equal or better performance

Note: Quantities provided are indicative and are intended for sizing purposes. Bidders remain responsible for validating the design and proposing the appropriate number, capacity, and architecture of distribution switches required to meet NHBRC's performance, resilience, and growth requirements throughout the contract term.

B4. WAN CONNECTIVITY REQUIREMENTS (INDICATIVE)

The WAN connectivity requirements provided below represent the NHBRC's current operational baseline and are intended to guide bidder sizing and solution design.

The table below provides indicative **WAN Sizing & Bandwidth Recommendations** requirements per site based on current user volumes and expected usage.

#	Site Name	Clients (Users and Devices)	WAN 1 Primary	WAN 2 Secondary
1	Sunninghill Head Office	643	150 Mbps	150 Mbps
2	Nelspruit	112	20 Mbps	20 Mbps
3	Durban	100	30 Mbps	30 Mbps
4	Century City	85	30 Mbps	30 Mbps
5	Polokwane	69	20 Mbps	20 Mbps
6	Rustenburg	62	20 Mbps	20 Mbps
7	Pretoria	54	20 Mbps	20 Mbps
8	Port Elizabeth	52	30 Mbps	30 Mbps
9	Eric Molobi	50	20 Mbps	20 Mbps
10	Bloemfontein	38	20 Mbps	20 Mbps
11	East London	32	30 Mbps	30 Mbps
12	George	30	20 Mbps	20 Mbps
13	Kimberley	25	20 Mbps	20 Mbps
14	Klerksdorp	22	20 Mbps	20 Mbps
15	Bethlehem	22	20 Mbps	20 Mbps
16	Witbank	21	20 Mbps	20 Mbps
17	Modimolle	18	20 Mbps	20 Mbps
18	Mahikeng	14	20 Mbps	20 Mbps
19	Richards Bay	13	20 Mbps	20 Mbps
20	Thulamela Municipality	11	20 Mbps	20 Mbps
21	Tzaneen	10	20 Mbps	20 Mbps
22	Newcastle	Future Site / Currently Unoccupied	20 Mbps	20 Mbps

Note: NHBRC reserves the right to increase, decrease, relocate, or establish additional sites during the contract period. The proposed WAN solution shall be capable of accommodating such changes through a flexible and scalable service model.

B5. LAN SIZING & UPLINK CLASSIFICATIONS

- The LAN uplink requirements provided below are indicative and are based on the NHBRC's current site sizes, user populations, and operational requirements.
- Bidders shall utilise these requirements as a minimum baseline when designing the proposed Local Area Network (LAN) infrastructure.
- The proposed solution shall be designed to support current operational demands while accommodating future growth, increased user density, evolving application requirements, and emerging technologies.

Indicative LAN Uplink Classification

Site	Estimated Clients (Users and devices)	Minimum LAN Uplink Requirement
Sunninghill Head Office	643	Minimum 10 Gbps redundant core uplinks with 1 Gbps or higher access switch uplinks
Nelspruit	112	Minimum 1 Gbps uplinks between access and distribution layers
Durban	100	Minimum 1 Gbps uplinks between access and distribution layers
Century City	85	Minimum 1 Gbps uplinks between access and distribution layers
Polokwane	69	Minimum 1 Gbps uplinks between access and distribution layers
Rustenburg	62	Minimum 1 Gbps uplinks between access and distribution layers
Pretoria	54	Minimum 1 Gbps uplinks between access and distribution layers
Port Elizabeth	52	Minimum 1 Gbps uplinks between access and distribution layers
Eric Molobi	50	Minimum 1 Gbps uplinks between access and distribution layers
Bloemfontein	38	Minimum 1 Gbps uplinks between access and distribution layers
East London	32	Minimum 1 Gbps uplinks between access and distribution layers
George	30	Minimum 1 Gbps uplinks between access and distribution layers
Kimberley	25	Minimum 1 Gbps uplinks between access and distribution layers
Klerksdorp	22	Minimum 1 Gbps uplinks between access and distribution layers
Bethlehem	22	Minimum 1 Gbps uplinks between access and distribution layers
Witbank	21	Minimum 1 Gbps uplinks between access and distribution layers
Modimolle	18	Minimum 1 Gbps uplinks between access and distribution layers
Mahikeng	14	Minimum 1 Gbps uplinks between access and distribution layers
Richards Bay	13	Minimum 1 Gbps uplinks between access and distribution layers
Thulamela Municipality	11	Minimum 1 Gbps uplinks between access and distribution layers
Tzaneen	10	Minimum 1 Gbps uplinks between access and distribution layers
Newcastle	Future Site / Currently Unoccupied	Minimum 1 Gbps uplinks between access and distribution layers

Note: The client counts provided are indicative only and are intended for sizing purposes. Bidders shall conduct their own assessment and propose appropriate switch capacities, uplink speeds, stacking technologies, port densities, and redundancy mechanisms to ensure optimal performance throughout the contract period. NHBRC reserves the right to increase or decrease user numbers and site requirements during the contract term, and the proposed solution shall accommodate such changes without requiring a fundamental redesign of the LAN architecture.

B6. DESIGN CONSIDERATIONS

Bidders must take into account the following:

- Network design must support current operations and projected growth
- Head Office shall be supported by high-throughput infrastructure (10Gbps or higher)
- Branch sites must be provisioned with reliable and scalable access-layer connectivity
- Wireless infrastructure must align with user density and access requirements
- The solution must support redundancy, resilience, and automatic failover
- The service provider shall implement SD-WAN or equivalent technology to optimise traffic routing
- Quality of Service (QoS) must prioritise Microsoft 365, Teams Voice, and critical SAP applications
- All edge devices must support encrypted throughput aligned to recommended bandwidth
- The solution must include proactive monitoring and SLA-based reporting
- The proposed design must support scalability of at least 30%–50% over the contract period

ANNEXURE C MANAGED HOSTING IAAS

Bidders must complete all pricing schedules (Annexures C–F) in full.

Any omissions, incomplete sections, or inconsistencies may result in disqualification

C1. PRICING INSTRUCTIONS

- All pricing must be in ZAR (South African Rand)
- All prices must be VAT inclusive
- Pricing must be fixed for Year 1
- Escalation for Years 2–5 must be clearly indicated (if applicable)
- Pricing must align with the proposed technical solution and architecture
- No additional, hidden, or unquoted costs shall be accepted after contract award unless formally approved through NHBRC's change control process.
- Bidders must provide a transparent and detailed breakdown of all costs.

C2. RECURRING MANAGED SERVICES PRICING

Service Component	Monthly Cost (ZAR Incl. VAT)	Annual Cost (ZAR Incl. VAT)
Compute / Virtual Machines		
Storage (Primary / Backup / Archive)		
Operating Systems / Platform Services		
Managed Hosting Services		
Service Management (Hosting Layer)		
TOTAL HOSTING COST		

C3. IMPLEMENTATION & TRANSITION (ONCE-OFF COSTS)

If applicable

Item	Unit of Measure	Unit Cost (ZAR Incl. VAT)
Additional User (All Services Including Identity, Access, Collaboration, and Management Services)	Per user / month	
Storage (All-Tier Storage: Primary, Backup, Archive where applicable)	Per GB / month	
Bandwidth (WAN / Internet / Cloud Connectivity as applicable)	Per Mbps / month	
Compute / Virtual Machine (Including CPU, RAM, Operating System, and Platform Services)	Per instance / month	

ANNEXURE D NETWORK CONNECTIVITY

Pricing Table: Bidders must comply with the following requirements when calculating their price.

Note: All prices must be inclusive of VAT.

D1. NETWORK SERVICES

Cost Component	Monthly Cost (ZAR Incl. VAT)	Annual Cost (ZAR Incl. VAT)
WAN Connectivity (Primary Links – MPLS / Internet / SD-WAN Underlay)		
WAN Connectivity (Secondary / Failover Links – Diversity Required)		
LAN Infrastructure Services (Switching, Access Layer, Distribution, Wi-Fi, Cabling Management)		
Network Security Services (Firewalls, IDS/IPS, SD-WAN Security, Secure Access Controls)		
Internet Connectivity Services (Business Internet Breakout, Redundant Internet Services, Bandwidth Management)		
Total Monthly Cost		
Total Annual Cost		

D2. NETWORK SERVICES TOTAL

Contract Year	Annual Cost (ZAR Incl. VAT)	Escalation (%)
Year 1		
Year 2		
Year 3		
Year 4		
Year 5		
Total Five-Year Contract Value		

ANNEXURE E	UNIFIED COMMUNICATIONS
-------------------	-------------------------------

E1. MICROSOFT TEAMS VOICE

Service Component	Monthly Cost (ZAR Incl. VAT)	Annual Cost (ZAR Incl. VAT)
Teams Voice Licensing		
Call Routing / Auto Attendant / IVR		
Call Analytics & Reporting		
SIP Trunking / PSTN Connectivity		
Support & Maintenance		
Total Voice Cost		
Total Annual Cost		

E2. MICROSOFT TEAMS VOICE TOTAL

Contract Year	Annual Cost (ZAR Incl. VAT)	Escalation (%)
Year 1		
Year 2		
Year 3		
Year 4		
Year 5		
Total Five-Year Contract Value		

F1. IMPLEMENTATION & TRANSITION (ONCE-OFF)

Cost Component	Quantity	Once-Off Cost (ZAR Incl. VAT)
Project Initiation & Design	1	
Migration / Transition Services	1	
Testing & Validation	1	
Training & Skills Transfer	1	
Cutover & Go-Live Support	1	
TOTAL ONCE-OFF COSTS		



ANNEXURE G

TOTAL COST SUMMARY (5 YEARS)

G1 TOTAL COSTS

Cost Category	Year 1 (ZAR Incl. VAT)	Year 2	Year 3	Year 4	Year 5	5-Year Total
Managed Hosting (IaaS)						
Network Connectivity						
Security Services						
Backup & DR						
Service Management						
Microsoft Teams Voice						
Implementation & Transition (Once-Off)		0	0	0	0	
TOTAL COST Excluding VAT						
TOTAL COST Including VAT						

G2 CHECKLIST

Requirement	Compliant (Y/N)	Comments
All pricing inclusive of VAT		
Year 1 pricing fixed		
Escalation clearly defined		
No hidden costs		
Aligned to technical solution		
Variable rates provided		
Once-off costs included		

The bidder MUST take note of the following:

- *The pricing schedule must be duly signed by the bidder/ and or a duly authorized individual by way of resolution which must be attached to the bid, if there is no signature on the pricing schedule the bidder will be disqualified.*
- *An incomplete pricing schedule will result in the bidder being disqualified, no alterations can be made subsequent to submission of the bid.*
- **PRICE ADJUSTMENTS:** *Bidders must take note that firm prices will be accepted for the first twelve (12) months of the contract duration, thereafter a once-off price adjustment on the 13th month will be accepted based on the average CPI % as issued by STATS SA.*
- All prices must be VAT Inclusive and must be quoted in South African Rand (ZAR).

NB: The Service Provider should carry their own travel and accommodation costs (if any)



Pricing Table: Bidders must comply with the following requirements when calculating their price.

Note: All prices must be inclusive of VAT.

REFER TO ANNEXURES C TO G

Bidder Signature	Total cost for five (5) years (incl. VAT) R

The bidder **MUST** take note of the following:

- The pricing schedule must be duly signed by the bidder and/ or a duly authorized individual by way of resolution which must be attached to the bid, **if there is no signature on the pricing schedule the bidder will be disqualified.**
- An incomplete pricing schedule will result in the bidder being disqualified, no alterations can be made subsequent to submission of the bid.
- **PRICE ADJUSTMENTS:** Bidders must take note that firm prices will be accepted for the first twelve (12) months of the contract duration, thereafter a once-off price adjustment on the 13th month will be accepted based on the average CPI % as issued by STATS SA.
- All prices must be VAT Inclusive and must be quoted in South African Rand (ZAR).

NB: The Service Provider should carry their own travel and accommodation costs (if any).

11. The table below is an approximate count. Bidders may assume a growth of 20% per office

Office Location	No. of Users
Sunninghill Head Office	214
Eric Molobi	11
Pretoria	28
George	7
East London	25
Kimberley	10
Richards Bay	7
Newcastle	7
Polokwane	18
Port Elizabeth	23
Tzaneen	21
Modimolle	4
Cape Town	45
Mafikeng	11
Bloemfontein	17
Nelspruit	20
Rustenburg	20
Klerksdorp	8
Bethlehem	12
Witbank	16
Durban	42
Thulamela	6

J1. PURPOSE

This Annexure defines the terminology, abbreviations, and acronyms used within this Request for Proposal (RFP), Scope of Work, and associated contractual documentation to ensure a common understanding between the NHBRC and prospective bidders.

J2. GLOSSARY OF TERMS

Term	Definition
Bidder / Service Provider	Any organisation or consortium submitting a proposal in response to this RFP.
Contract	The formal agreement entered into between NHBRC and the successful bidder.
Data Centre	A physical facility used to house computer systems, servers, storage, networking equipment, and associated ICT infrastructure.
Disaster Recovery (DR)	The process, policies, and procedures to recover and protect ICT infrastructure and data following a disruption or disaster.
Business Continuity (BCP)	The ability of the organisation to maintain critical business operations during and after a disruption.
Hosting Services	Provision of infrastructure (compute, storage, and networking) for running NHBRC systems and applications.
Managed Services	The practice of outsourcing day-to-day management of ICT infrastructure and services to a third-party provider.
Service Level Agreement (SLA)	A formal agreement defining expected service performance levels, including availability, response times, and resolution timelines.
Migration	The process of transferring systems, data, and services from the current environment to a new environment.
High Availability (HA)	The design and implementation of systems to ensure minimal downtime and continuous service availability.
Scalability	The ability of the system to handle increased workloads by adding resources without impacting performance.
Resilience	The ability of ICT systems to withstand and recover from failures or disruptions.
Proof of Concept (PoC)	A demonstration used to validate the feasibility of a proposed solution.
Total Cost of Ownership (TCO)	The total cost of a solution over its lifecycle, including capital and operational expenses.
Availability	The percentage of time that a system or service remains operational and accessible to users.
Backup	The process of creating copies of data to enable recovery in the event of data loss, corruption, or disaster.
Bandwidth	The maximum data transfer capacity of a network connection measured in Mbps or Gbps.
Business Continuity	The capability of the organisation to continue delivering critical services during and after a disruption.
Cloud Computing	Delivery of computing services including servers, storage, networking, software, and databases over the internet.
Commissioning	The formal process of testing, validating, and placing systems into operational service.
Defence-in-Depth	A layered cybersecurity strategy that applies multiple security controls across infrastructure, applications, networks, and users.

Demilitarised Zone (DMZ)	A segmented network area used to host public-facing systems while isolating internal networks from external access.
Endpoint Detection and Response (EDR)	Security technology used to detect, investigate, and respond to threats on servers, workstations, and endpoints.
Failover	Automatic switching to a standby system, network, or infrastructure component when the primary component fails.
High Availability	Infrastructure and systems designed to minimise downtime and ensure continuous service availability.
Hosting Environment	The infrastructure platform used to run applications, databases, and ICT services.
Infrastructure-as-a-Service (IaaS)	A cloud or hosted service model providing virtualised computing resources such as servers, storage, and networking.
Incident	An unplanned interruption or degradation of an ICT service.
Load Balancing	Distribution of workloads or network traffic across multiple systems to optimise performance and availability.
Malware	Malicious software designed to disrupt, damage, or gain unauthorised access to systems or data.
Monitoring	Continuous observation and analysis of infrastructure, applications, and network services to ensure operational health.

J3. ACRONYMS

Acronym	Meaning
AAD	Azure Active Directory
API	Application Programming Interface
AWS	Amazon Web Services
BAC	Bid Adjudication Committee
BCDR	Business Continuity and Disaster Recovery
BCP	Business Continuity Plan
BEC	Bid Evaluation Committee
CAB	Change Advisory Board
CAPEX	Capital Expenditure
CCTV	Closed-Circuit Television
CPI	Consumer Price Index
CSI	Continuous Service Improvement
CVI	Cloud Video Interoperability
DID	Direct Inward Dialling
DMZ	Demilitarised Zone
DR	Disaster Recovery
DRaaS	Disaster Recovery as a Service
EDR	Endpoint Detection and Response
Gbps	Gigabits per second
IaaS	Infrastructure as a Service
IAM	Identity and Access Management
ICT	Information and Communication Technology
IDS	Intrusion Detection System
IPS	Intrusion Prevention System
IPSec	Internet Protocol Security
ISO	International Organization for Standardization
ITIL	Information Technology Infrastructure Library
IVR	Interactive Voice Response
KPI	Key Performance Indicator
LAN	Local Area Network
MFA	Multi-Factor Authentication
MPLS	Multi-Protocol Label Switching

MTTR	Mean Time to Restore
NGFW	Next-Generation Firewall
NHBRC	National Home Builders Registration Council
OLA	Operating Level Agreement
OPEX	Operational Expenditure
PaaS	Platform as a Service
PoE	Power over Ethernet
POP	Point of Presence
POPIA	Protection of Personal Information Act
PSTN	Public Switched Telephone Network
QoS	Quality of Service
RBAC	Role-Based Access Control
RCA	Root Cause Analysis
RFP	Request for Proposal
RPO	Recovery Point Objective
RTO	Recovery Time Objective
SaaS	Software as a Service
SAP	Systems, Applications and Products
SD-WAN	Software-Defined Wide Area Network
SIEM	Security Information and Event Management
SIP	Session Initiation Protocol
SLA	Service Level Agreement
SOC	Security Operations Centre
TIA	Telecommunications Industry Association
UPS	Uninterruptible Power Supply
VDI	Virtual Desktop Infrastructure
VLAN	Virtual Local Area Network
VM	Virtual Machine
VoIP	Voice over Internet Protocol
VPN	Virtual Private Network
WAF	Web Application Firewall
WAN	Wide Area Network
Wi-Fi	Wireless Fidelity
ZAR	South African Rand