NATIONAL HOME BUILDING

NHBRC®

REGISTRATION COUNCIL

ASSURING QUALITY HOMES

Terms of Reference

NATIONAL HOME BUILDING

NHBRC®

REGISTRATION COUNCIL

ASSURING QUALITY HOMES

REQUEST FOR PROPOSALS FOR THE APPOINTMENT OF A MANAGED CYBERSECURITY SERVICES PROVIDER FOR A PERIOD OF FIVE (05) YEARS

RFP NO.:	NHBRC 01/2026
CLOSING DATE:	10 SEPTEMBER 2026
TIME:	11:00
BID SUBMISSION	https://www.etenders.gov.za/

VIRTUAL NON-COMPULSORY BRIEFING SESSION

DATE:	28 August 2026
TIME:	11:00

VENUE: https://teams.microsoft.com/l/meetup-join/19%3ameeting_YTVjZDdkMDctZjc4OS00NjQ1LTgxMTAtNjZjYzY0YWEzYTIi%40thread.v2/0?context=%7b%22Tid%22%3a%223fa2c7f2-3ceb-4b67-aec9-08d186f26abc%22%2c%22Oid%22%3a%2202f62474-c23f-4de8-9b08-853046ec1257%22%7d

1. TERMS AND CONDITIONS

1.1. This Request for Proposal (RFP) has been compiled by the NHBRC, and it is made available to the Bidders on the below 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 620 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. TERMS OF REFERENCE

5.1. PURPOSE

5.1.1. The NHBRC seeks to appoint a suitably qualified and experienced Managed Cybersecurity Services Provider (MCSP) for a period of five (05) years to deliver comprehensive, end-to-end cybersecurity services. The TOR defines scope, objectives, service requirements, performance expectations, and governance arrangements for services across NHBRC's national network of offices.

- Strengthen NHBRC's security posture and resilience through a defence-in-depth approach.
- Provide 24/7/365 monitoring, detection, triage, containment, and incident response.
- Reduce cyber risk exposure through continuous exposure management and remediation support.
- Support compliance with ISO/IEC 27001, POPIA, PFMA and relevant internal policies.
- Improve cybersecurity maturity through assessments, governance uplift, and continuous improvement.
- Enhance security culture through cyber awareness and human-risk management.

5.2. BUSINESS DRIVERS

5.2.1. The NHBRC is on a digital transformation journey aimed at improving business operations and enhancing service delivery to the South African public.

5.2.2. As NHBRC increasingly relies on digital platforms, cloud services, and integrated systems, safeguarding information assets requires robust cybersecurity controls that extend beyond traditional ICT infrastructure to encompass users, data, applications, and third-party integrations.

5.2.3. The NHBRC recognises that cybersecurity is a specialised and evolving discipline and therefore requires a strategic partner to complement existing internal ICT and information security capabilities over 5 years.

5.2.4. The organisation seeks to assess and improve its cybersecurity posture using internationally recognised standards and frameworks, enabling a clear understanding of current risk exposure and maturity levels.

5.2.5. The engagement aims to support the progressive improvement of cybersecurity controls, governance, and operational maturity through structured assessments, continuous monitoring, and advisory services.

5.3. OBJECTIVES

5.3.1. The engagement aims to implement **a managed cybersecurity services model** that:

5.3.1.1. Strengthens NHBRC's security posture and resilience.

5.3.1.2. Enhances threat detection, prevention, and response capabilities.

5.3.1.3. Ensures compliance with ISO/IEC 27001, POPIA, PFMA, and other relevant regulatory and best-practice frameworks.

5.3.1.4. Provides 24/7/365 Security Operations Centre (SOC) monitoring and incident handling.

5.3.1.5. Protects sensitive data and prevents data leakage.

5.3.1.6. Improves NHBRC's overall cybersecurity maturity.

5.4. CURRENT NHBRC IT ENVIRONMENT

5.4.1. NHBRC operates a hybrid environment supported by contracted service providers. The following is indicative and may be refined during onboarding:

- Cloud and hosted services (including Microsoft Azure and other third-party hosted services).
- Microsoft 365 tenant with E3 and E5 licensing.
- Perimeter security, including FortiGate firewall and VPN capability (e.g., OpenVPN).

- Approx. 650 workstations; approx. 300 tablets (Windows and iOS); Cisco switching; network printers.

Note: Bidders must propose solutions that integrate with and/or optimize NHBRC's existing environment, or propose alternatives with clear justification, migration approach, and cost impacts.

5.5. GUIDING PRINCIPLES

5.5.1. Technology integration: bidders may propose any mature, industry-recognised security technologies and architectures that integrate with the existing environment.

5.5.2. Co-managed transparency: runbooks, playbooks, detections, dashboards, and operational artefacts must be visible to NHBRC; no black-box operations.

5.5.3. Security-by-design: align to MITRE ATT&CK, ISO/IEC 27001, NIST CSF and relevant NIST publications, OWASP, and CIS Benchmarks.

5.5.4. Compliance-first: controls and processes must support POPIA, PFMA, and NHBRC policy requirements.

5.5.5. Cost transparency: provide full cost model including telemetry/logging, retention, automation, licensing, and optimisation measures.

5.5.6. Data sovereignty: SOC operations and analyst access for NHBRC data must be based in South Africa.

5.6. SCOPE OF WORKS

5.6.1. The MCSSP shall deliver end-to-end managed cybersecurity services across people, process, and technology. Detailed technical requirements are contained in Annexure A.

5.6.1.1. Defence-in-Depth (Layered Security) Requirements

a) The bidder must implement and operate a layered security design covering, at minimum, the following layers:

b) Cloud security (posture management, workload protection, cloud logging, cloud identity and privilege security).

c) Network security (perimeter controls, segmentation, IDS/IPS, secure remote access, DNS and network anomaly detection).

d) Server and infrastructure security (hardening, patching, workload monitoring, EDR/XDR coverage, privileged access controls).

e) Application security (secure SDLC integration, SAST/DAST/SCA, API security testing, WAF where applicable, secrets management).

f) Database security (encryption, auditing, activity monitoring, privilege oversight, vulnerability assessment and patching).

g) Identity and access security (MFA, RBAC, adaptive controls, PAM/JIT/JEA, service account governance).

h) Endpoint/device security (EDR/XDR, hardening, encryption, removable media controls, mobile device/app management).

i) Data security (classification, DLP, rights management, retention/records, insider risk considerations).

5.6.2. 24/7/365 Security Operations Centre (SOC)

5.6.2.1. Provide 24/7/365 monitoring, detection, triage, containment, response coordination, and reporting across identities, endpoints, email/collaboration, cloud, applications, network, and data.

a) Operate SIEM/SOAR capabilities suitable for enterprise monitoring, case management, and automation; integrate with NHBRC log sources.

b) Operate EDR/XDR capabilities to support investigation and response actions across endpoints and identities.

c) Deliver a use-case catalogue mapped to MITRE ATT&CK; implement and tune detections to reduce false positives.
d) Provide runbooks/playbooks (automated and analyst-driven), including rollback steps, escalation and approvals.
e) Provide proactive threat hunting (weekly baseline hunts and monthly deep hunts) and deliver reusable queries/content.
f) Provide operational resilience for SOC operations (redundancy, business continuity, secure communication channels).

5.6.3. Incident Response (IR) and Forensics

a) Maintain IR playbooks aligned to NIST incident handling, including decision trees per incident type (e.g., ransomware, BEC, identity compromise, data exfiltration, application breach, cloud compromise).
b) Provide an IR retainer with surge capacity and defined SLAs; on-site support within agreed timelines for high-severity incidents.
c) Provide forensic capability with chain-of-custody, evidence preservation, and investigation reporting suitable for audit and legal review.
d) Support POPIA-aligned breach communications, including draft regulator and data-subject notification packs where required.
e) Provide post-incident RCA reports, corrective action plans, and detection/playbook improvements.

5.6.4. Vulnerability Assessment and Penetration Testing

a) Conduct vulnerability scanning (authenticated where feasible) across endpoints, servers, network devices, cloud workloads, and applications.
b) Provide exposure prioritisation using exploitability context and business criticality; maintain a remediation tracker and dashboards.
c) Conduct penetration testing at least annually for internal and external environments and at least semi-annually for web/app/API; include retesting within 30–60 days post-remediation.
d) Provide executive and technical reports including evidence, CVSS scoring, and remediation guidance.

5.6.5. Threat Intelligence (TI)

a) Provide actionable threat intelligence using relevant sources (commercial, open-source, industry sharing), mapped to MITRE ATT&CK.
b) Correlate TI with SIEM/XDR detections and implement IOC/IOA updates within agreed timeframes.
c) Provide periodic intelligence briefings and monthly threat landscape reports tailored to NHBRC and the South African threat context.

5.6.6. (ASM/CTEM) Attack Surface Management / Continuous Threat Exposure Management (ASM/CTEM)

a) Provide external attack surface monitoring and asset discovery, including shadow IT detection where feasible.
b) Provide continuous threat exposure management (CTEM) outputs: exposure scoring, attack-path insights (where supported), and prioritised remediation roadmaps.
c) Provide credential exposure monitoring and integrate exposure insights into SOC prioritisation and reporting.

5.6.7. Data and Document Security

5.6.7.1. The MCSSP must support data protection controls and secure document handling for sensitive NHBRC documents (e.g., invoices, statements, enrolment certificates). Requirements include:

a) Document-level protection such as encryption and/or password protection for sensitive documents, with policies aligned to NHBRC access control standards.
b) Secure external sharing controls, including restrictions on forwarding/printing/copying where required by policy.

c) Audit logging for document access, modification, and sharing events, and integration of relevant events into monitoring where feasible.

5.6.8. Cyber Awareness and Human Risk Management

a) Deliver an annual cyber awareness programme with role-based training aligned to NHBRC risks and user groups.

b) Conduct phishing simulations at least quarterly and provide metrics (click rate, report rate, repeat offenders) and targeted coaching.

c) Provide executive briefings and periodic awareness reporting.

5.6.9. Policy Development and Governance Uplift

a) Develop/update a Cyber Incident Response Plan (CIRP) and supporting playbooks and communications plans.

b) Develop/update a Third-Party Access and Supplier Security Policy (onboarding, access controls, reviews, monitoring).

c) Develop/update a SOC Engagement Plan defining RACI, escalation, communications, approval points, and governance forums.

d) Develop/update policies for identity and privileged access, vulnerability and patch management, acceptable use, and data classification/retention.

5.7. DELIVERABLES

5.7.1. The bidder shall deliver the following, without duplication across sections. Detailed templates are included in Annexures:

a) Onboarding pack: architecture and data-flow diagrams, log source register, RACI, escalation matrix, communications plan, and onboarding schedule.

b) Operational artefacts: SOC runbooks and IR playbooks, use-case catalogue, detection tuning notes, and automation/playbook catalogue.

c) Reporting: daily/weekly operational summaries, monthly KPI and risk posture report, quarterly executive maturity and improvement roadmap.

d) Assurance outputs: risk and maturity assessment with roadmap; updated cybersecurity risk register.

e) Testing outputs: vulnerability reports, penetration testing reports, and retest evidence.

5.7.2. Training outputs: awareness programme artefacts, phishing simulation reports, attendance records, and knowledge transfer completion evidence.

5.8. ROLES AND RESPONSIBILITIES

5.8.1. Responsibilities of the Bidder

5.8.1.1. Ensure secure deployment, monitoring, and management of cybersecurity tools.

5.8.1.2. Always maintain the confidentiality of NHBRC data.

5.8.1.3. Provide dedicated, skilled cybersecurity resources.

5.8.1.4. Ensure compliance with cybersecurity best practices and standards.

5.8.1.5. Maintain incident logs, dashboards, documentation, and audit trails.

5.8.1.6. Deliver services according to the SLA.

5.8.2. Responsibilities of NHBRC

5.8.2.1. Provide access to relevant systems, networks, and environments.

5.8.2.2. Share existing security policies and risk register.

5.8.2.3. Participate in joint incident response activities.

5.8.2.4. Provide timely approvals where required.

5.9. SERVICE LEVELS AND KPIs

5.9.1. Minimum service levels are as follows (bidders may propose stronger targets)

Table 1: Service Level KPIs

Metric	Target	Notes
24/7 SOC Coverage	100%	Continuous monitoring and on-call capability.
P1 MTTD	≤ 15 minutes	Time from alert generation to human triage.
P1 MTTR (Containment)	≤ 2 hours	Time from triage to containment action completion.
P2 Triage	≤ 30 minutes (95%)	High-priority incident triage performance.
Critical Vulnerability Remediation	≤ 7 days	From verified detection to remediation/mitigation or approved exception.
Reporting Timeliness	100%	Delivery of agreed reports on schedule.

5.10. SOC LOCATION AND DATA SOVEREIGNTY

5.10.1. The bidder must maintain a fully operational 24/7/365 SOC located within the Republic of South Africa.

5.10.2. All analyst access to NHBRC monitoring data, alerts, and incident case information must be performed from within South Africa, unless explicitly approved in writing by NHBRC.

5.10.3. The bidder must describe SOC physical security controls, resiliency, and continuity arrangements.

5.11. BIDDER MINIMUM REQUIREMENTS

a) Minimum five (5) years proven experience delivering enterprise-grade managed cybersecurity services.

b) Demonstrable operational capability to provide 24/7/365 SOC services.

c) Valid ISO/IEC 27001:2022 certification applicable to the bidder’s managed security services/SOC environment.

d) Valid ISO 9001 Certificate for a Quality Management System

e) Minimum three (3) contactable reference letters for similar MCSSP engagements.

f) Qualified resources with relevant certifications and experience across SOC, IR/forensics, cloud security, IAM, and governance.

g) Disclosure of SOC location(s) in South Africa, data handling practices, and any subcontractors/sub-processors.

6. TECHNICAL DATA TO BE SUBMITTED BY THE BIDDER

6.1. REQUIRED TECHNICAL SUBMISSION

6.1.1. The NHBRC requires bidders to submit a detailed technical and capability-based proposal/submission demonstrating their ability to deliver enterprise-grade Managed Cybersecurity Services (MCSSP) in line with the scope and requirements of these Terms of Reference (TOR). Refer to Annexure A

6.1.2. The submission must demonstrate proven operational capability, supported by verifiable evidence, and not merely theoretical frameworks or generic documentation.

6.2. EXPERIENCE AND OPERATIONAL CAPABILITY

6.2.1. The bidder must have a minimum of five (5) years’ proven experience in delivering enterprise-grade Managed Cybersecurity Services.

6.2.2. The bidder must demonstrate experience in servicing public sector entities or similarly regulated organisations within South Africa.

6.2.3. The bidder must demonstrate the operational capability to provide 24/7/365 managed cybersecurity services, including a functional Security Operations Centre (SOC).

6.3. CERTIFICATIONS, STANDARDS, AND COMPLIANCE

6.3.1. The bidder must provide evidence of a valid ISO/IEC 27001:2022 certification applicable to its Security Operations Centre (SOC) or managed security services environment.

6.3.2. The bidder must demonstrate alignment with recognised cybersecurity frameworks, including NIST Cybersecurity Framework and/or COBIT.

6.4. TECHNOLOGY PLATFORM AND OEM AUTHORISATION

6.4.1. The bidder must provide proof of OEM certifications/letter, advanced partner status, or authorised reseller/managed service agreements for security technologies to be procured or licensed by the bidder, including but not limited to:

- SIEM / XDR
- Endpoint Detection and Response (EDR)
- Network and perimeter security
- Cloud security platforms

6.4.2. The bidder must ensure that the certification/letter is up to date and maintained before and after the appointment by the NBHRC.

6.4.3. Evidence must confirm that the bidder is authorised to deploy, operate, and support the proposed technologies.

6.5. RESOURCE CAPABILITY AND QUALIFICATIONS

6.5.1. The bidder must assign dedicated cybersecurity resources to the NHBRC contract.

6.5.2. Key personnel must collectively demonstrate experience in:

- Security Operations (SOC)
- Incident Response and Digital Forensics
- Network and Cloud Security (Microsoft Azure)
- Identity and Access Management
- Governance, Risk, and Compliance

6.5.3. Assigned resources must hold relevant industry certifications, including but not limited to:

- CISSP
- CISM
- GCIH / GCFA
- OSCP
- Microsoft Security Certifications

6.5.4. A concise CV must be provided for each proposed resource, clearly indicating role, certifications, and relevant experience.

6.6. CLIENT REFERENCES AND PROVEN DELIVERY

6.6.1. Completed MCSSP Projects

6.6.1.1. The bidder must demonstrate successful delivery of Managed Cybersecurity Services by submitting a summary of completed or active MCSSP engagements.

6.6.1.2. The summary must be presented in the following format and must correspond directly with the reference letters submitted:

Project Name	Project Description	Project Period (Start – End)	Contract Value (incl. VAT)	Client Name	Client Contact

6.7. REFERENCE LETTERS

6.7.1. A minimum of three (3) contactable reference letters must be provided.

6.7.2. Reference letters must:

- Be on the client's official letterhead
- Be signed by an authorised representative
- Confirm the scope and duration of MCSSP services delivered
- Include client contact details for verification

Note: *Reference letters must relate to cybersecurity services of similar scope and complexity to the NHBRC requirement.*

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).

***Note:* Please attach a reference letter from the client indicating the successful completion of the project as per the client's brief. (Excluding the NHBRC)**

6.8. CAPABILITY OF BIDDER'S RESOURCES

6.8.1. The bidder must demonstrate that proposed resources have experience in similar MCSSP or enterprise cybersecurity environments.

6.8.2. Experience must include, but is not limited to:

- SOC operations and monitoring
- Incident detection and response
- Cyber threat intelligence
- Vulnerability and penetration testing
- Cloud and endpoint security management

6.9. PROJECT PROPOSAL AND IMPLEMENTATION APPROACH

6.9.1. The bidder must submit a detailed project proposal outlining the implementation and transition to managed services.

6.9.2. The proposal must include:

- Implementation phases and milestones
- Platform onboarding and integration approach
- Risk and change management approach
- Knowledge transfer and capacity-building plan

6.9.3. The bidder must acknowledge that some activities may be required outside normal business hours to avoid disruption to NHBRC operations.

6.9.4. NHBRC reserves the right to request replacement of any resource that does not meet SLA performance expectations, subject to written approval.

7. TECHNICAL AND PRICE EVALUATION CRITERIA

7.1. BID EVALUATION

7.1.1. In accordance with the NHBRC Supply Chain Management Policy, the bid evaluation process shall be carried out in three (03) stages, namely:

7.1.1.1. Stage 1: Compliance check of bid requirements.

7.1.1.2. Stage 2: Functional Evaluation Criteria (Stage 2A paper-based: 80 points; Stage 2B live SOC demonstration: 20 points).

7.1.1.3. Stage 3: Price and Preference Points Evaluation

7.2. MINIMUM QUALIFYING THRESHOLD TO PROCEED TO STAGE 3: 80 POINTS OUT OF 100 (COMBINED STAGE 2A + STAGE 2B)

7.3. 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.

7.3.1. Bidders must comply with all mandatory administrative requirements to qualify for further evaluation *(failure to comply will result in a disqualification of the bid)*

MANDATORY DOCUMENTS TO BE SUBMITTED FOR DISQUALIFICATION		
No.	**Bidders shall take note of the following bid conditions / Mandatory Submissions**	**Yes/No**
1.	**Pricing Schedule** – Must be completed and signed, including a detailed cost breakdown and escalation per annum. Must be signed by the bidder or an authorised individual (with resolution attached). *If not signed, the bidder will be disqualified.*	
2.	**SBD 4** – Bidders Disclosure Form must be fully completed and signed	
3.	Bidders must provide a valid **ISO 27001** Certificate for an Information Security Management System**.** The bidder must ensure that the certification is up to date and maintained before and after the appointment by the NBHRC. Online verification to be made by NBHRC.	
4.	Bidders must provide a valid **ISO 9001** Certificate for a Quality Management System. The bidder must ensure that the certification is up to date and maintained before and after the appointment by the NBHRC. Online verification to be made by NHBRC.	
5.	Bidders must provide a valid **Cyber Security Professional Indemnity and/or Cyber Liability Insurance** to a minimum coverage amount of R 10 000 000.00 (Ten Million Rand). The bidder must provide a certified copy of the insurance certificate or policy schedule and must remain valid for the full duration of the contract, with evidence of renewal provided to NHBRC.	

7.3.2. Bidders must comply with all mandatory administrative requirements to qualify for further evaluation

LEGISLATIVE DOCUMENTS TO BE SUBMITTED NOT FOR DISQUALIFICATION		
No.	**Bidders shall take note of the following bid conditions / Mandatory Submissions.**	Yes/No
1.	**SBD 1** – Invitation to Bid completed and signed	
2.	**SBD 3.1** – Pricing Schedule (Firm Price) completed	
3.	**SBD 6.1** – Preference Claim Form completed and signed (even if no points claimed)	
4.	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	

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

7.4. STAGE 2: FUNCTIONALITY EVALUATION

7.4.1. Evaluation Criteria

- Bids must **fully comply with all Mandatory Requirements** from **Stage 1 (Mandatory Compliance Check)**.
- Any bid failing Stage 2 – Part A requirements will be **invalidated or disqualified**.

7.4.1. Stage 2 – Part A – Paper-Based Technical Evaluation

- **Purpose:** Assess documented capability and evidence (experience, references, certifications, solution fit).
- Total Points: **80**

- Only bidders who scored Stage 2A (≥60) are invited to Stage 2B.

7.4.2. Stage 2 – Part B – Live Demo Site Visit (Verification & Practical Assessment)

- **Purpose:** Verify that the proposed MCSSP solution and team can deliver in practice and validate claims made in Stage 2. A.
- Maximum: **20 points.**
- **Minimum threshold to qualify for the Final Technical Score is ≥10 points.**

7.4.3. Final Technical Score (FTS)

- FTS = Stage 2A Score + Stage 2.B score
- Maximum: 100 points.
- To proceed to Stage 3 (price and preference), bidders must achieve an FTS of at least 80 (including scoring a minimum of 10 points in Stage 2B).

7.4.3. The Bidders' information will be scored according to the following point systems:

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

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

No.	Evaluation Criteria	Description	Weight
1	**Bidder's Experience**	The bidder **MUST** have at least five (05) years' proven track record implementing, supporting, and maintaining MCSSP/managed cybersecurity for enterprise customers. Please attach a company profile that includes a list of MCSSP projects with scope, timelines, technologies, and outcomes that demonstrate relevant experience. **Bidder Experience** 0 Years' Experience = 0 Points 1 Year Experience = 1 Point 2 Years' Experience = 2 Points 3 Years' Experience = 3 Points 4 Years' Experience = 4 Points 5 Years' Experience and more = 5 Points	**10**
2	**Client Reference Letters**	The bidder **MUST** provide positive written contactable reference letters for the projects listed in their profile. <u>The reference letters from the clients of a bidder MUST include:</u> 1. Company name 2. Company letterhead 3. Contact person and contact telephone numbers 4. Signature of duly authorized person 5. The period during which the project was executed	**20**

		6. The client reference letters must be relevant to the NHBRC requirements. **Scoring Allocation** 0 Reference letter = 0 Points 1 Reference letter = 1 point 2 Reference letters = 2 Points 3-4 Reference letters = 3 Points 5 Reference letters = 4 Points 6 Reference letters and more = 5 Points **NB: Reference letters must correspond directly to the claimed bidder's experience above**	
3	**Project Team Capability**	The bidder **MUST** provide an **organogram for the entire project** team with clearly defined roles as listed below. For the required roles below, provide **qualifications**, **certifications, and comprehensive CVs**. Points are awarded only for submissions meeting all minimum requirements. **Scoring Allocation:** Total = (Sum of points/total of 12 points) **Required Roles & Minimum Requirements:** **1. Project Manager (Maximum points =3)** • **NQF level 7** qualification or equivalent in any field. **(Max 1 point)** • Project Management Professional Certification (PMP) or PRINCE2 (Practitioner) or Certified Scrum Master (CSM) or MPI-ACP (Agile Certified Practitioner). **(Max 1 point)** • An abridged CV indicating a minimum of 5 years' ISO 27001 implementation experience. **(Max 1 point)** **2. Chief Information Security Officer (Maximum points =3)** • **NQF 7** in computer science or information and communication technology-related qualification. **(Max 1 point)** • **Certification** in Certified Information Systems Security Professional (CISSP) or Certified Chief Information Officer (CCSIO) or Certified Information Security Manager (CISM) or CompTIA Advanced Security Practitioner (CASP+) **(Max 1 point**) • **An abridged CV** indicating a minimum of 5 years' experience managing cybersecurity-related projects. **(Max 1 point)** **3. Security Operation Centre (SOC) lead (Maximum points =3)**	**30**

		• **NQF 7** in Computer Science, Cyber Security, or Information and Communication Technology related qualification. **(Max =1 point)** • **Certified** in Security+ and CompTIA CySA+ and Certified Ethical Hacker (CEH) **(Max =1 point)** • **An abridged CV** indicating a minimum of 5 years of technical and management experience in SOC and/or in the field. **(Max =1 point)** **4. <u>Cyber Security Architect (Maximum points =3)</u>** • **NQF 7** in Computer Science, Cyber Security, or Information and Communication Technology related qualification **(Max =1 point)** • **Certification** in Certified Information Systems Security Professional (CISSP) or Certified Information Security Manager (CISM) or Certified Cloud Security Professional (CCSP) and SABSA or TOGAF/ Microsoft Certified; Cybersecurity Architect Expert or GIAC certifications, i.e., GDSA **(Max =1 point)** • **An abridged CV** indicating a minimum of 5 years' experience in cybersecurity-related projects**. (Max =1 point)**	
4	**Migration Plan**	The Service Provider **MUST submit** a project plan must include objectives, scope, timelines, resources, Risk Management, and work breakdown structure and a methodology confirming the understanding of the scope of work, including process flows, timelines of six months, and deliverables which **must be relevant to the NHBRC** requirements. **Note: Bidders must submit the project plan, methodology, process flows, timelines and deliverables.** **<u>Scoring Allocation</u>** Bidder failed to submit a project plan, methodology, process flows, timelines, and deliverables = **0 Points.** Bidder submitted 1 item of the migration plan requirements = **1 Point**. Bidder submitted 2 items of the migration plan requirements **= 2 Points.** Bidder submitted 3 items of the migration plan requirements = **3 Points.** Bidder submitted 4 items of the migration plan requirements **= 4 Points.** Bidder submitted 5 items of the migration plan requirements **= 5 Points**	**20**
SUBTOTAL			**80 Points**
MINIMUM QUALIFYING REQUIREMENT			**60 Points**

NB: Only bidders who score 60 points or more out of 80 points (Stage 2 Part A) will qualify for Site Presentation Evaluation (Part B)

7.4.4. Stage 2 Part B – Live SOC Demonstration (20 points)

i. The NHBRC requires shortlisted bidders to participate in a Mandatory Live Security Operations Centre (SOC) Demonstration as part of the technical evaluation process.

ii. The demonstration will be conducted after the closure of bids and will be limited to bidders who have met all administrative and minimum technical compliance requirements.

iii. The purpose of the demonstration is to verify the bidder's actual MCSSP operational capability, including:

   a. Live SOC operations,
   b. Security tooling in active use
   c. Incident detection and response workflows
   d. Reporting and governance practices

iv. The demonstration must be conducted using the bidder's own operational SOC environment (physical or virtual) and must not be a simulated, conceptual, or marketing demonstration.

v. Bidders shall demonstrate:

   a. A live SIEM/XDR dashboard populated with real (redacted) data
   b. Active incident workflows and playbooks
   c. Analyst investigation processes
   d. SOC escalation and reporting mechanisms

vi. Failure to participate in the mandatory demonstration, or demonstration of a non-operational or simulated environment, shall result in disqualification.

vii. The live SOC demonstration does not replace paper submissions but serves as verification of claims made in the bid response.

7.4.4.1. Standard Demo Scoring Guide (Applied Per Criterion)

Score	Description
5 – Excellent	Fully live demonstration using operational systems; seamless integration; clear runbooks; measurable KPIs; strong evidence of maturity
4 – Very Good	Mostly live demonstration; minor gaps or limited simulation
3 – Good	Adequate demonstration; some reliance on screenshots or partial simulation
2 – Average	High reliance on slides; limited hands-on capability
1 – Poor	Minimal working demonstration; significant gaps
0 – Non-compliant	Fails to demonstrate the requirement

7.4.4.2. **Live SOC Demonstration – Scoring Matrix (20 Points)**

No.	Criterion	What Will Be Verified	Score
1	**SOC Architecture & Integration**	Live walkthrough of the MCSSP systems/architecture and how it integrates with enterprise components similar to NHBRC, including: • Firewalls • Endpoints, servers, networks, etc. • SIEM/XDR and SOAR Verification will include: • Log ingestion and data flows • Policy enforcement points • Visibility through dashboards • Supporting artefacts (architecture and data-flow diagrams, screenshots)	**5**
2	**Incident Detection & Response**	Demonstration of live SOC operations, including: • Alert triage and correlation logic • Automation (SOAR) workflows • Escalation paths, RACI, and handover procedures • Evidence of operational metrics (e.g., MTTA, MTTR reporting)	**5**
3	**Endpoint & Identity Controls**	Demonstration of: • Endpoint Detection & Response (EDR) remediation actions • Endpoint compliance and encryption status • MFA and SSO enforcement • Privileged Access Management (PAM) workflows (e.g. JIT access, approvals) • Identity and device compliance dashboards	**3**
4	**Vulnerability & Patch Management**	Evidence of: • Vulnerability scanning and reporting • Risk scoring and prioritization • Patch orchestration workflows • Exception handling and tracking • Management or executive-level reports	**2**
5	**Compliance, Data Protection & Reporting**	Demonstration of: • Alignment of SOC processes to POPIA and ISO 27001 • Data encryption and key management practices • Data recovery workflows • Sample compliance, audit, or assurance reports used in active environments	**5**
	TOTAL		**20 Points**

7.4.5. Bidders who score a total of 80 points or more on two stages (Paper-based and live Demo Evaluation) will qualify for further evaluation, which is the Price and Preference Points system.

7.4.6. The minimum threshold for functionality is 80 points or greater 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.

7.5. STAGE 3: PRICE AND PREFERENCE POINTS EVALUATION

7.5.1. Only bids that obtained a minimum qualifying score **(80 points)** for **Stage 2 (Functional Requirements)** will be evaluated further.

7.5.2. The contract will be awarded in terms of Regulations 4 of the Preferential Procurement Regulations about the Preferential Procurement Policy Framework Act, 2000 (Act 5 of 2000), and the Preferential Procurement Regulations, 2022, and bids will be adjudicated in terms of the (80/20) preference points system. Points are awarded to bidders based on the below:

80/20 Preference point system (for the acquisition of services, works, or goods with a Rand value not more than R 50 million) (all applicable taxes included)

$$P_S = 80\left(1 - \frac{P_t - P_{min}}{P_{min}}\right)$$

Where;

P_s = Points scored for the comparative price of the bid or offer under consideration

P_t = Comparative price of the bid or offer under consideration

P_{min} = Comparative price of the lowest acceptable bid or offer.

7.5.2.1. The points scored will be rounded off to the nearest two decimal places.

7.5.2.2. The points will be awarded to a Bidder in accordance with the table below:

7.5.2.2.1. A maximum of 20 points may be awarded to a bidder for Preference Points specified in the tender.

Preference Points	Points Allocated
Women	12
Youth	6
Disabilities	2
Military Veterans	0
TOTAL	**20 Points**

7.5.2.3. The following formula must be applied to calculate the number of points for preference points

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

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

7.5.2.4. The points scored for price will be added to the points scored for preference points to obtain the Bidders total points scored out of 100 points.

8. AVAILABILITY OF THE RFP DOCUMENT

8.1. 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 **19 August 2026.**

8.2. There will be a non-compulsory virtual briefing session that will be held on **28 August 2026 at 11h00** *(Should Prospective Bidders who wish to attend the briefing session virtually struggle to connect on the day, an email should be sent to tenders@nhbrc.org.za to request an invite before 11:00).*

8.3. Link for virtual non-compulsory briefing session:

8.3.1. The link can also be accessed on the NHBRC website: **https://teams.microsoft.com/l/meetup-join/19%3ameeting_YTVjZDdkMDctZjc4OS00NjQ1LTgxMTAtNjZjYzY0YWEzYTli%40thread.v2/0?context=%7b%22Tid%22%3a%223fa2c7f2-3ceb-4b67-aec9-08d186f26abc%22%2c%22Oid%22%3a%2202f62474-c23f-4de8-9b08-853046ec1257%22%7d**

9. RFP CLOSING DATE

9.1. RFP Proposal should be marked for Attention: Supply Chain Manager and submitted online via National Treasury eTender Portal (https://www.etenders.gov.za/) on or before **10 September 2026 at 11h00**.

9.2. **No physical or emailed RFP proposals will be accepted.**

9.3. **No late submissions will be accepted**.

10. VALIDITY PERIOD OF BIDS

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

11. ENQUIRIES DIRECTED TO

11.1. The administrative enquiries may be directed to:

Department: Supply Chain Management

Contact Person: Mr Kabelo Phalane

E-mail address: Kabelo@nhbrcsa.onmicrosoft.com

11.2. Clarifications and enquiries should be sent to Kabelo@nhbrcsa.onmicrosoft.com, tenders@nhbrc.org.za up to 03 September 2026. Responses will be communicated during weekdays, between Monday and Friday from 8:30 am to 16:30 pm.

11.3. Responses will be communicated during weekdays, between Monday and Friday from 8:30 am to 16:30 pm.

11. SUBMISSION OF PROPOSALS

11.1. ONLINE BID SUBMISSION

11.1.1. Bidders must submit their bids online in a PDF format through the e-Tender Publication portal.

11.1.2. The online e-Tender publication portal can be accessed at the following link: https://www.etenders.gov.za/

11.1.3. The guide for online bid submission is attached. **https://youtu.be/B7pNseNJYHM**

11.1.4. 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.

For identification purposes are requested to ensure that proposals contain the company's details and are easily identifiable by company logo or name.

11.1.5. Non-compliance with online bid submission WILL invalidate the bidder’s response.

11.1.6. 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.

12. DISCLAIMER

12.1. DUE DILIGENCE

12.2. The State reserves the right to:

12.2.1. 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.

12.2.1.1. 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.

12.2.1.2. Conduct any evaluation verifications prior to final award or at any time during the contract term period.

12.3. NEGOTIATIONS

12.3.1. 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.

12.4. RIGHT OF AWARD

12.4.1. The State reserves the following rights –

12.4.2. Not to make any award in this bid or accept any bids submitted,

12.4.3. Appoint one service provider

12.4.4. Request further technical information from any bidder after the closing date,

12.4.5. Verify information and documentation of the bidder(s),

12.4.6. 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.

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

12.5. APPOINTMENT OF BIDDERS

12.5.1. 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.

12.6. FRONTING

12.6.1. 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.

12.6.2. 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.

12.6.3. 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.

12.7. RESPONSIVE BIDS

12.7.1. 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.

12.8. TERMS AND CONDITIONS

12.8.1. 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.

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

13. POPIA

13.1. 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.

13.2. 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.

13.2.1. 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)

13.2.2. 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.