

Terms of Reference

Provision of IT Infrastructure Hosting Services for a Government Agency

Vista Resources Integrated Consultancy Limited is pleased to invite vendors to submit a proposal for the provision of infrastructure hosting services covering compute, storage, network security, load balancing, backup, and disaster recovery for a Government Agency's digital health systems. These include the electronic Community Health Information System (eCHIS), the national Electronic Medical Records (EMR) platform, and supporting applications such as OpenLMIS, DHIS2, the application suite, and Dashboard.

Vista is not prescribing a specific infrastructure delivery model for this engagement. Firms may propose colocation, public cloud, private cloud, a hybrid arrangement, on-premises hardware supply with managed services, or any other model, provided the proposal meets the requirements set out in this document. Section 5 requires each firm to state and justify the delivery model it is proposing.

1. Background and Rationale

The Agency's digital health systems currently run across a combination of on-premises servers at its headquarters and virtual machines hosted with a third-party provider. An internal technical assessment of this environment identified a combined production workload of 44 virtual machines, together with a series of some infrastructure gaps

These gaps if left unaddressed could result in service outage, data loss, or other concerns. This engagement forms part of the Agency's broader effort to consolidate its infrastructure into a secure, resilient, professionally managed environment, migrated in a phased manner that preserves service continuity throughout.

2. Objectives of the Assignment

- Provide a secure, resilient hosting environment for consolidated compute and storage workload.
- Deliver a phased, low-risk migration that preserves ability to roll back at each stage until the migrated workload is validated in production.
- Provide a fully costed, transparent commercial structure that supports budgeting, audit, and public procurement requirements.

Specifically, the engaged firm will be expected to:

- Host the Agency's full consolidated workload which currently consists of 44 virtual machines across on-premises and third-party-hosted environments
- Provide dedicated network security, load balancing, and backup services
- Stand up a disaster recovery environment at a separate site from the primary hosting facility, with defined recovery targets.
- Provide multi-carrier internet connectivity with automatic failover
- Support projected annual infrastructure growth over the life of the engagement.

3. Current Infrastructure Overview

The firm should size its proposed solution against current consolidated workload, summarised below, with headroom for projected annual growth (see Section 5):

- Cluster 1: 18 virtual machines, 109 vCPU, 202.2 GB RAM, 8.66 TB storage.
- Cluster 2: 26 virtual machines, 307 vCPU, 1,372 GB RAM, 21.355 TB storage.
- Consolidated total: 44 virtual machines, 416 vCPU, approximately 1.54 TB RAM, approximately 30.02 TB storage.

A detailed, system-level inventory will be shared with shortlisted firms under a mutual non-disclosure agreement.

4. Scope of Work

Infrastructure Provisioning and Design

- Design and provision infrastructure, using the firm's proposed delivery model, sized to at least 416 vCPU and 1,574.2 GB RAM of effective compute capacity, with a minimum 25 percent growth buffer and at least N+1 redundancy.
- Provision at least 40 TB of production-grade storage, with a clearly costed path to expand capacity (priced per GB or per the firm's standard unit of measure).
- Disclose the sizing methodology used. For example, vCPU-to-physical-core ratio and RAM oversubscription policy for a virtualised model, or equivalent sizing logic for a public cloud, hybrid, or on-premises model.

Security and Resilience

- Deploy a dedicated, highly-available next-generation firewall (or equivalent) at the network edge, including intrusion prevention/detection, web application firewall capability, and distributed denial-of-service mitigation.
- Deploy a dedicated, highly-available load balancing tier in front of public and internal applications, with health-check-based routing and SSL offload.
- Provide centralised security logging with an exportable feed suitable for SIEM integration and NDPA compliance reporting.
- Provide backup infrastructure that is physically separate from production compute, with a minimum 30-day retention period and periodic restore testing.

Migration and Cutover

- Migrate non-production (UAT/staging) workloads first, to validate connectivity, performance, and cutover procedures.
- Migrate on-premises production workloads, maintaining rollback capability at each step.
- Migrate the currently externally-hosted workload estate into the same governed environment.
- Complete final DNS/IP cutover and decommission legacy infrastructure no longer required, in coordination with the Agency.

Disaster Recovery

- Stand up a disaster recovery environment at a separate site from the primary hosting site.
- Replicate the Agency's core production database and application servers to the disaster recovery site, with defined and stated Recovery Time Objective (RTO) and Recovery Point Objective (RPO) targets.

- Conduct periodic, documented disaster recovery failover testing.

Ongoing Operations and Support

- Provide 24x7x365 monitoring and incident response for the hosted environment.
- Provide multi-carrier internet connectivity (minimum two independent ISPs) with automatic, DNS-independent failover.
- Provide quality-of-service-based bandwidth segmentation between public-facing and internal traffic.

5. Technical and Commercial Requirements

Firms must respond to each requirement below, indicating full compliance, partial compliance, or non-compliance, with supporting explanation for any partial or non-compliant response. Proposals that do not address a requirement will be treated as non-compliant for that item.

- State clearly the infrastructure delivery model being proposed. For example, colocation, public cloud, private cloud, hybrid, on-premises hardware supply with managed services, or another model and include the rationale for that choice given specified requirements in Sections 3 and 4.
- State a guaranteed uptime SLA (percentage) and the remedy or service credit applicable if that SLA is breached.
- State the minimum contract period, billing cycle, whether billing is in advance or arrears, and whether quoted prices are inclusive or exclusive of VAT.
- State explicitly who holds ownership/title of the underlying infrastructure under the proposed model, whether that is the Agency, the firm, or a hybrid arrangement, and describe what happens to the hardware and Agency's data at contract end or early termination.
- Provide a fully itemised pricing schedule covering compute, storage (including any overage beyond a bundled allocation), backup, network security, load balancing, disaster recovery, IP allocation, internet bandwidth, and any one-time setup or licensing costs.
- Describe the process, timeline, and any associated cost for extracting the Agency's data and workloads at contract end.
- Confirm compliance with the Nigeria Data Protection Act (NDPA) 2023 and provide a draft Data Processing Agreement.

6. Duration & Reporting

The hosting arrangement itself is expected to run on an ongoing basis, subject to the contract term proposed by the firm and agreed with the Agency.

The firm will work closely with our technical team throughout the migration and subsequent hosting period. Regular reporting and coordination meetings will be mandatory to ensure alignment with operational and compliance requirements.

7. Qualifications and Experience Required

- Valid Corporate Affairs Commission (CAC) registration in Nigeria, current tax clearance certificate, and evidence of good standing with the Bureau of Public Procurement (BPP), where applicable.
- Demonstrable experience hosting mission-critical infrastructure for government, health-sector, or comparably regulated clients, with at least two verifiable reference sites.

- Evidence of data centre certification or an equivalent operational standard, such as a recognised uptime tier certification or ISO/IEC 27001.
- Evidence of financial capacity to deliver and sustain the proposed service, such as a bank reference or audited financial statements for the last two years.

8. Proposal Submission Requirements

Prospective firms are expected to submit a full proposal package that includes:

- A detailed technical proposal outlining the understanding of the assignment, proposed architecture, methodology, and migration plan.
- A financial proposal with a clear, itemised breakdown of costs, addressing every requirement in Section 5.
- A completed compliance matrix responding to every requirement in Sections 4 and 5.
- Organisational profile and CVs of key personnel highlighting relevant qualifications and experience.
- Evidence of similar assignments previously conducted, including reports, references, or contracts.

Proposals will be evaluated on technical compliance, fit of the proposed delivery model to the Agency's requirements, proposed migration approach, vendor experience and references, service level commitments, and total cost of ownership over the life of the contract.

Submission Guidelines

All applications must be submitted electronically to vistaprocuramentad@gmail.com on or before 31st August 2026. The subject of the email shall be "IT Infrastructure Hosting Services Engagement." Submissions that fail to comply with these guidelines will not be considered.