an agency of the
Department of Arts and Culture

TERM OF REFERENCE **26 March 2021**

Bid NO: SAHRA/NIU/21/04/2021

THE SOUTH AFRICAN HERITAGE RESOURCES AGENCY (SAHRA) INVITES ALL SUITABLY QUALIFIED CLOUD SERVICE PROVIDERS TO SUBMIT PROPOSALS FOR THE PROVISION OF CLOUD HOSTING SERVICES FOR ITS ICT APPLICATIONS AND INFRASTRUCTURE

1. PURPOSE

1.1. The South African Heritage Resources Agency (SAHRA) herewith intends to appoint a suitable and reputable supplier for the provision cloud hosting services for a period of two (2) years for the SAHRA.

2. BACKGROUND

2.1. SAHRA's current ICT infrastructure is hosted across multiple environments some owned and run by SAHRA and others owned and run by third parties. The off-premises hosting providers are SAGE, AWCAPE and IS Ignite. The on-premises server rooms are in Cape Town and Pretoria. The infrastructure has both physical and virtualized environments.

2.2. The Cloud Services Provider will have to consolidate, lift, and shift, optimize and provide cloud backup and restore services for all services and endpoints.

2.3. One of the core applications at SAHRA, with the biggest workload, is an online heritage resource database, and heritage management tool, known as the South African Heritage Resources Information System (SAHRIS). The application was developed in 2011 and launched publicly in April 2013. The system was developed on a free, open-source platform, Drupal, in compliance with Section 39 of the National Heritage Resources Act, 25 of 1999.

2.3.1. Section 39 (1) stipulates that: For the purposes of the consolidation and co-ordination of information on heritage resources, SAHRA must compile and maintain an inventory of the national estate, which must be in the form of a data base of information on heritage resources which it considers to be worthy of conservation... and for this purpose it must co-ordinate, and may prescribe, national standards for the recording of information by provincial heritage authorities.

2.3.2. The system facilitates this mandate in several ways. Firstly, it acts as a heritage sites repository, recording and archiving all known recorded heritage sites in the country, be these derived from extant museum and university survey records, or from field researchers conducting Heritage Impact Assessments. Secondly, SAHRIS is a heritage collections management tool. This means the system can store digital copies of registers of objects and collections, and monitor and manage their conservation, condition, and movement. Thirdly, the system manages the process of heritage management as stipulated in the NHRA, by allowing for heritage comments and permits to be applied for by the public, reviewed by heritage officers and commented on or permitted online. Through

these functions, the system enables the efficient and coordinated management of South African heritage and maximizes the benefit that can be attained from our heritage resources by appropriate promotion and use of these resources.

2.3.3. The online accessibility of the system makes it freely available to all members of the public, while also opening South African heritage to the world.

3. SCOPE OF WORK

The South African Heritage Resources Agency (SAHRA) wishes to engage a Managed CSP to provide Cloud Hosting Services for a period of 2 years. The details of the ICT infrastructure and applications are provided on Annexure-A below. The scope of the project will cover the following services:

3.1. ENVIRONMENT REQUIREMENT:

a) Infrastructure as Service (IaaS) - Migration of all the applications and websites listed in Annexure-A and hosting of applications and website.

b) An environment for the deployment of applications/websites in Annexure-A. The hosting service will:

- Cloud staging environment
- Cloud production environment

Each of the environments mentioned above should be logically isolated, i.e., the Staging environment will be in a different virtual private cloud (VPC) than the production environment and setup will be such that users of the environments are in separate networks.

The CSP shall be responsible for provisioning required compute infrastructure (server/virtual machines), storage as the indicative compute requirements in the commercial Bid, in built AntiSpam/Malware/Antivirus threats control software etc.

3.2. MIGRATION OF EXISTING APPLICATIONS:

a) Migration of applications and the websites will be responsibility of the CSP supported by SAHRA's ICT staff.

b) The CSP will support the migration process including VM configuration, installation and configuration of the operating systems, network and VPC Zone creation and configuration etc.

3.3. OPERATIONS & MAINTENANCE SERVICES

a) Resource Management

- Adequately size the necessary compute, memory, and storage required, building the redundancy into the architecture (including storage) and load balancing to meet the service levels.
- While the initial sizing & provisioning of the underlying infrastructure may be carried out based on the information provide in the Annexure-C. Subsequently, it is expected that the bidder, based on the growth in the user load (peak and non-peak periods; year-on-year

increase), will scale up or scale down the compute, memory, and storage as per the performance requirements of the solution.

- For any major expected increase in the workloads, carry out the capacity planning in advance to identify & provision, where necessary, the additional capacity to meet the user growth and/or the peak load requirements to support the scalability and performance requirements of the solution. Range of Upward Auto-Scaling is 70% CPU utilisation.
- The scaling up / scaling down (beyond the auto-scaling limits or whenever the auto-scaling limits must be changed) must be carried out with prior approval by SAHRA. The CSP shall provide the necessary details including the sizing calculations, assumptions, current workloads & utilisations, expected growth / demand and any other details justifying the request to scale up or scale down.

b) Patch & Configuration Management

- Manage the instances of storage, compute instances, and network environments. This includes department-owned & installed operating systems and other system software that are outside of the authorisation boundary of the CSP. CSP is also responsible for managing specific controls relating to shared touch points within the security authorisation boundary, such as establishing customised security control solutions. This work will include, but are not limited to, configuration and patch management, vulnerability scanning, disaster recovery, and protecting data in transit and at rest, host firewall management, managing credentials, identity, and access management, and managing network configurations.

c) User Administration

- Management of users in the OS level and firewall level will be taken care of by CSPs.
- Properly separates users by their identified roles and responsibilities, thereby establishing least privilege and ensuring that users have only the permissions necessary to perform their assigned tasks.

d) Security Administration

- Appropriately configure the security groups in accordance with the SAHRA networking policies.
- Regularly review the security group configuration and instance assignment to maintain a secure baseline.
- Secure and appropriately segregate / isolate data traffic/application by functionality using DMZs, subnets etc.
- Ensure that the cloud infrastructure and all systems hosted on it, respectively, are properly monitored for unauthorised activity.
- Properly implementing anti-malware and host-based intrusion detection systems on their instances, as well as any required network-based intrusion detection systems in accordance with SAHRA Security policies.

e) Monitoring Performance and Service Levels.

- Provide and implement tools and processes for monitoring the availability of assigned applications, responding to system outages with troubleshooting activities designed to identify and mitigate operational issues.
- Reviewing the service level reports, monitoring the service levels and identifying any deviations from the agreed service levels.
- Monitoring of service levels, including availability, uptime, performance, application specific parameters, e.g., for triggering elasticity, request rates, number of users connected to a service. See Annexure A
- Detecting and reporting service level agreement infringements.
- Monitoring of performance, resource utilisation and other events such as failure of service, degraded service, availability of the network, storage, database systems and operating Systems including API access within the cloud service provider's boundary.

f) Usage Reporting and Billing Management

- Track system usage and usage reports
- Monitoring, managing, and administering the monetary terms of SLAs and other billing related aspects.
- Provide the relevant reports including real time as well as past data/information/reports to validate the billing and SLA related penalties.
- Provide the Access Log report

g) Backup

- Configure, schedule, monitor and manage backups of all the data including application and database but not limited to files, images, and databases as per the policy finalized by SAHRA Manipur.
- Restore from the backup where required.

h) Business Continuity Services

- Provide business continuity services in case the primary site becomes unavailable.

i) Support for third party audits

- Ensure that logs and audit trails are enabled and stored for audit purpose.

j) Miscellaneous

- Advise on optimal operational practices, recommend deployment architectures for cloud infrastructures, design and implement automated scaling processes, day-to-day and emergency procedures, deploy and monitor underlying cloud services, performance reporting and metrics, and ensure the overall reliability and responsive operation of the underlying cloud services through both proactive planning and rapid situational response.

3.4. EXIT MANAGEMENT / TRANSITION-OUT SERVICES

a) Provide a comprehensive exit management plan.

b) Migration of the VMs, data, content, and any other assets to the new environment or on alternate cloud service provider's offerings and ensuring successful deployment and running of SAHRA's solution on the new infrastructure by suitably retrieving all data, scripts, software, virtual machine images, and so forth to enable mirroring or copying to SAHRA supplied industry standard media.

c) Ensure that all the documentation required for smooth transition including configuration documents are kept up to date.

d) Once the exit process is completed, remove the data, content and other assets from the cloud environment and destroy the VM, Content and data of SAHRA.

e) Ensure that all the documentation required by SAHRA for smooth transition are kept up to date and all such documentation is handed over to SAHRA during regular intervals as well as during the exit management process.

f) Support and assist SAHRA for a period of three months so that the SAHRA can successfully deploy and access the services from the new environment.

g) Train and transfer the knowledge to SAHRA staff to ensure similar continuity and performance of the Services post expiry of the Agreement.

Note: The ownership of the data generated upon usage of the system, at any point of time during the contract or expiry or termination of the contract, shall rest absolutely with SAHRA.

3.5. TECHNICAL FEATURES:

a) CSP must offer a service by which recommendations are made to the customer about configurations the customer can make to optimize their financial spend with the provider. The service must provider customer-specific recommendations based on current or historical patterns at the provider and must not be customer-generic. Recommendations must be actionable, tied to specific assets and documented as having a certain amount of financial savings. This service must be offered directly by the provider and not require the customer to seek third-party partners.

b) Relational DBaaS

- CSP must offer a relational database as a service (DBaaS), provided as a fully automated, self-service turnkey offering. In this service, the customer should not have access to the underlying instance, and the database maintenance must be done entirely by the provider. At a minimum, the service must support two open-source databases (either MySQL or PostgreSQL). CSP must offer relational DBaaS in a locally redundant fashion, meaning that the customer database is automatically replicated across multiple data centers within a single geography.

c) Local identity management and granular role-based authorization

- Cloud Service Providers must include, at minimum, a local identity management system (that is, local accounts) with granular role-based authorization for network services in both the service interfaces and management console. At a minimum, the role-based authorization must support assigning authorization based on individual users and groups of users and delineation must be assignable per firewall, load balancer, IP address and network segment and support, as applicable, the following granular actions: create, delete, and configure.

d) Security Information and Event Management

- CSP may also propose a product or provide a service, turnkey offering by which SAHRA can configure real-time analysis and alerting of security events. At a minimum, service must support alerting, log retention and some form of forensic analysis that is able to search across logs and periods of time for patterns.

e) Customer VPN connectivity

- CSP must allow customers to access the cloud service via an IPsec VPN tunnel or Secure Sockets Layer (SSL) VPN tunnel over the public Internet. This must be a self-service capability from the provider side, although customers will have to make configurations on their end.

f) Encryption services

- The block and object storage services must offer self-service ability from both management console and Command Line Interface to opt into provider-enabled server-side encryption (SSE) for objects or object hierarchies within the storage service.

g) Bulk data import/export with encryption

- CSP must provide a portable storage device for bulk data import/export. SAHRA must be able to encrypt the data prior to transport and then decrypt it upon arrival. The encryption service must be built into the storage device and not left to the SAHRA.

4. LICENSING AGREEMENTS

4.1. The subscription software licenses that are coupled with the Infrastructure within scope are deemed included as part of the asset sale. These include the Operating System and Security software.
4.2. Virtualisation, backup, and storage software will be offered for use by the Cloud Services Provider.
4.3. The Bidder is responsible for paying support and maintenance fees for these licences. These fees will be offset during monthly billing. Conversely the Cloud Services Provider will supply their own virtualisation, backup and storage software at their own cost and pay support fees.
4.4. Hardware maintenance and support will be the responsibility of the Bidder for the duration of the contract. Both the licenses and hardware maintenance and support agreements will be deemed included as part of the asset sale provided it is within the bounds of the legal contract with the current OEMs/vendors.

5. GENERAL ROLES AND RESPONSIBILITIES:

The following services will be the responsibility of the CSP:

5.1. Operations and administration services are the activities associated with the day-to-day management of the cloud IaaS computing environment.

- They provide and support a stable infrastructure and effectively and efficiently perform operational and processing procedures to ensure services meet SLA targets.
- It also includes job scheduling and execution activities e.g., for scheduling of batch jobs.

5.2. Maintenance and Refresh Services roles and responsibilities

- Maintenance and Refresh services are the preventative maintenance activities performed to ensure that IaaS service is stable and will not fail. It also includes the operational activities needed to support SAHRA's ongoing development and project activities.
- This service includes hardware and software maintenance, OS, hypervisor etc.
- It also includes activities needed to ensure that SAHRA's Servers are configured in accordance with SAHRA's Policies and directions.

5.3. Cloud Computing Services roles and responsibilities

- Cloud computing services are the activities associated with the provisioning of compute resources on the cloud platform.
- The activities associated with the operations, administration, and management of the cloud computing environment.
- The maintenance activities performed to ensure that cloud computing environment is stable and will not fail.

5.4. Storage and data management services roles and responsibilities:

- Storage and data management services are the activities associated with the provisioning and day-to-day management of the installed storage and data environment.
- These include direct access storage devices (DASD), redundant array of independent disks (RAID), storage area network (SAN), network-attached storage (NAS), and tape and optical.
- They provide a stable support infrastructure and effectively and efficiently perform procedures to ensure services meet SLR targets and requirements.
- It also includes the activities associated with the day-to-day management of the backup environment including the associated backup media.

5.5. Cloud Storage and Data Management Services roles and responsibilities:

- Storage and data management services are the activities associated with the provisioning and day-to-day management of the installed storage and data environment.
- Providers must offer a wide variety of cloud storage, and these services are often complementary to a compute offering. Block and object storage services are the most common offerings found in the industry. Block storage services typically are not exposed via the internet, whereas object services typically are.
- They provide a stable support infrastructure and effectively and efficiently perform procedures to ensure services meet SLA targets and requirements.

5.6. Network Management:

- With respect to connectivity between the Cloud and SAHRA's Network, all network connections into SAHRA's Network will be established via a vendor neutral site.

5.7. Information Security Management Services roles and responsibilities:

Information Security Management Services provide security related services that cut across an organisation's business and IT environment to help safeguard and maintain the confidentiality, integrity, and availability of information.

This covers the following Information Security Management Services:

- The Patch Management Service provides for the distribution, management, monitoring and feedback function of patch updates throughout SAHRA's IT infrastructure environment, as per the contracted service. This Service applies to the server operating system level.
- The Anti-Malware Management Service provides for the distribution, centralised management, monitoring and feedback function of anti-malware signature files and updates throughout SAHRA's IT infrastructure environment, as per the contracted services. Antimalware includes, but is not limited to Anti-virus, Host Intrusion Detection and Prevention System, Host-based firewall and advanced persistent threat protection.
- The Vulnerability Management Service provides for identification, classification, remediation, and mitigation of vulnerabilities.
- The expert advice to SAHRA in respect of the various Information Security Services offered by the Cloud Service Provider in its security catalogue.

5.8. Incident and Problem Management:

- Incident and Problem Management service includes all the activities needed to actively resolve Incidents and to proactively close identified Problems.

5.9. Configuration Management:

- Configuration tracking service includes all the activities needed to ensure that Infrastructure assets and their configuration are properly tracked.

5.10. Capacity and Performance Management:

- Component and Capacity Management service aims to ensure that the capacity and performance of services running on the IaaS Platform can deliver in accordance with the agreed Target Service Levels in a cost effective and timely manner, within the agreed Performance Standards. SAHRA requires component level capacity and performance management to cover CPU, Memory, Network, etc.)

6. TERMS AND CONDITIONS

6.1. All costs and expenses incurred by potential service providers relating to their project proposal will be borne by each respective service provider. SAHRA is not liable to pay such costs and expenses or to reimburse or compensate service providers in the process under any circumstances, including the rejection of any proposal or the cancellation of this project.

6.2. While SAHRA endeavours to ensure that all information provided to all potential service providers is accurate, it makes no warranty as to the accuracy or completeness of any information provided by it.

6.3. SAHRA reserves the right to waive deficiencies in project proposals. The decision as to whether a deficiency will be waived or will require the rejection of a project proposal will be solely within the discretion of SAHRA.

6.4. SAHRA reserves the right to request new or additional information regarding each service provider and any individual or other persons associated with its project proposal.

6.5. SAHRA reserves the right not to make any appointment from the proposals submitted.

6.6. Service providers shall not make available or disclose details pertaining to their project proposal with anyone not specifically involved, unless authorized to do so by SAHRA.

6.7. Service providers shall not issue any press release or other public announcement pertaining to details of their project proposal without the prior written approval of SAHRA.

6.8. Service providers are required to declare any conflict of interest they may have in the transaction for which the tender is submitted or any potential conflict of interest. SAHRA reserves the right not to consider further any proposal where such a conflict of interest exists or where such potential conflict of interest may arise.

6.9. valid original tax clearance certificate, issued by the South African revenue services, must be submitted, failing which the relevant service provider's proposal shall not be considered. (see attached application form for tax clearance certificate)

6.10. All project proposals shall become the property of SAHRA and shall not be returned.

6.11. The proposals should be valid and open for acceptance by SAHRA for a period of 30 days from the date of submission.

6.12. Service providers are advised that submission of a project proposal gives rise to no contractual obligations on the part of SAHRA.

6.13. SAHRA reserves the right not to accept any proposal which does not comply with the terms of reference and conditions set out in the proposal documents.

6.14. SAHRA reserves the right not to award, or not award the proposal to the service provider that scores the highest points.

6.15. Disputes that may arise between SAHRA and a service provider must be settled by means of mutual consultation, mediation (with or without legal representation) or, when unsuccessful, in a South African court of law.

6.16. All returnable proposal documents must be completed in full and submitted together with the service provider's quote and a sample annual report book.

6.17. The "requirements for content of the project proposal" section above outlines the information that must be included in proposal offers. Failure to provide all or part of the information may result in your proposal being excluded from the evaluation process.

6.18. All goods/service or products to be supplied to SAHRA shall be in full compliance with South African approved standards and in compliance to the specifications provided.

6.19. It is the conditions of this BID that, a quotation is submitted together with the following completed forms; kindly submit fully completed bid documents.

a) SBD 1 Invitation Bid
b) SBD 2 Tax Clearance certificate application form
c) SBD 3.3 Pricing Schedule
d) SBD 4 Declaration of Interests form
e) SBD 6.1 Preference points claim form (valid BBBEE certificate must be submitted together with this completed document.
f) SBD 7.1 Contract Form – Rendering of Services
g) SBD 8 Declaration of Bidders SCM practices
h) SBD 9 Declaration of independent bid determination

i) General Conditions of Contract (Please initial each page)

j) Registration with National Treasury Supplier Database (CSD)

NB: Failure to submit original completed returnable forms as mentioned above will automatically disqualify your quotation.

SAHRA reserves the right to revise any aspect of these timeframes at any stage, and to amend the process at any stage.

7. ANNEXURE-A (INDICATIVE RESOURCES)

The pricing structure should be based on a 10% storage allocation increase per annum but only charged for actual growth.

Services

Name of service	O/S	Storage	RAM	vCPUs
SAHRIS - Apache2 Webserver, PHP, Virtualmin	Linux	30GB	2GB	2
SAHRIS - Apache Solr Indexing Server	Linux	10GB	0.5GB	2
SAHRIS – Geoserver	Linux	100GB	1GB	2
SAHRIS - Kobo Server	Linux	10GB	1GB	2
SAHRIS - RDS for PostgreSQL	N/A	20GB	1GB	2
SAHRIS - RDS for MySQL	N/A	20GB	2GB	2
Memcached server	N/A	N/A	16GB	N/A
Storage	N/A	2TB	N/A	N/A

TAB 1 – PHASE II – ICT INFRASTRUCTURE

Name of the service	O/S	Storage	RAM	vCPUs
Print server	Linux	20GB	8GB	2
ProcessMaker	Linux	929GB	8GB	2
Elastic File System	N/A	900 GB	N/A	N/A
Archiving Storage	N/A	1024 GB x 30	N/A	N/A
S3 Glacier	N/A	5TB	N/A	N/A
Data Transfer	N/A	100GB	N/A	N/A

Business Support

Service	Description
1	VPC
2	Directory services
3	Backup and replication services
4	Advanced DDOS protection
5	DNS Manager
6	IPSEC VPN Connections
7	Virtual Firewall instance and Subnet level
8	Anti-virus (per VM)
9	Content Delivery Network with Web Application firewall
10	Identity and Access management
11	Managed Threat detection
12	Cloud Management and Monitoring Dashboard
13	Audit trail logs
14	Security and encryption for data at rest and in transit

- ❖ Ability to take snapshots and restore these to images in a virtual cloud service environment.

8. PRICING SCHEDULE

TAB 1 – PHASE I – SAHRIS MIGRATION – PRICING

Name of service	O/S	Storage	RAM	vCPUs	Once Off Costs (ZAR)	Monthly Costs (ZAR)
SAHRIS – Apache2 Webserver, PHP, Virtualmin	Linux	30GB	2GB	2		
SAHRIS – Apache Solr Indexing Server	Linux	10GB	0.5GB	2		
SAHRIS – Geoserver	Linux	100GB	1GB	2		
SAHRIS – Kobo Server	Linux	10GB	1GB	2		
SAHRIS – RDS for PostgreSQL	N/A	20GB	1GB	2		
SAHRIS – RDS for MySQL	N/A	20GB	2GB	2		
Memcached server	N/A	N/A	16GB	N/A		
Storage	N/A	2TB	N/A	N/A		

TAB 1 – PHASE II – ICT INFRASTRUCTURE – PRICING

Name of the service	O/S	Storage	RAM	vCPUs	Once Off Costs ZAR	Monthly Costs ZAR
Print services	Linux	200GB	8GB	2		
ProcessMaker	Linux	929GB	8GB	2		
Elastic File System	N/A	900 GB	N/A	N/A		
Archiving Storage	N/A	1024 GB x30	N/A	N/A		
S3 Glacier	N/A	5TB	N/A	N/A		
Data Transfer	N/A	100GB	N/A	N/A		

TAB 2 – BUSINESS SUPPORT SERVICES PRICING

Service Description	Once Off Costs (ZAR)	Recurring Costs (ZAR)
PostgreSQL Service		
MySQL Service		
Directory services		

Content Delivery Network		
Backup and File services		
Advanced DDOS protection		
VPN Connections		
Virtual Firewall instance and Subnet level		
Web Application firewall		
Identity and Access management		
Cloud Management and Monitoring Dashboard		
Audit Trail logs		
Security and Encryptions for data at rest and in transit		

The Cloud Service Cost at are only indicative for price discovery. The payment shall be made only for actual pay per usage as per the relevant unit price of the selected CSP. CSP shall also provide for any requirement above the indicated. All changes will be discussed and agreed with SAHRA.

9. SERVICE LEVEL AGREEMENT (SLA)

Measurement and Monitoring

a) The SLA parameters shall be monitored on monthly basis as per the individual SLA parameter requirements. However, if the performance of the system/services is degraded significantly at any given point in time during the contract and if the immediate measures are not implemented and issues are not rectified to the complete satisfaction of SAHRA, then SAHRA will have the right to take services from another CSP at the cost of existing CSP or/and termination of the contract.
b) The full set of service level reports should be available to SAHRA monthly or based on the project requirements.
c) The CSP shall comply with relevant legislation, policies and standards including:
    - Protection of Personal Information
    - Information Security Standards e.g ISO 27000 series including ISO 27001 and 27017 and 27018.
    - Undergoing regular third-party audits including SOC2 audits
d) The Monitoring Tools shall play a critical role in monitoring the SLA compliance and hence will have to be customized accordingly. The CSP shall make available the Monitoring tools for measuring and monitoring the SLAs. The bidder may deploy additional tools and develop additional scripts (if required) for capturing the required data for SLA report generation in automated way. The tools should generate the SLA Monitoring report in the end of every month which is to be shared with the SAHRA. SAHRA shall have full access to the Monitoring Tools/portal (and any other tools/solutions deployed for SLA measurement and monitoring). SAHRA will also audit the tool and the scripts on a regular basis.
e) The measurement methodology/criteria/logic will be reviewed by SAHRA.

f) In case of default on any of the service level metric, the CSPs shall submit performance improvement plan along with the root cause analysis for SAHRA's approval.

Periodic Reviews

a) During the contract period, it is envisaged that there could be changes to the SLA, in terms of measurement methodology/logic/criteria, addition, alteration or deletion of certain parameters, based on mutual consent of both the parties, i.e., SAHRA and CSP.
b) SAHRA and CSP shall each ensure that the range of the Services under the SLA shall not be varied, reduced, or increased except by the prior written agreement of SAHRA and CSP in accordance with the Change Control Schedule.
c) The SLAs may be reviewed on an annual basis by SAHRA in consultation with the CSP.

Penalties

Payments to the CSP to be linked to the compliance with the SLA metrics laid down in the agreement.

d) The payment will be linked to the compliance with the SLA metrics (the SLA will be discussed and agreed with the winning bidder).
e) The penalty in percentage of the monthly Payment is indicated against each SLA parameter in the table.
f) In case multiple SLA violations occur due to the same root cause or incident then the SLA that incurs the maximum penalty may be considered for penalty calculation rather than a sum of penalties for the applicable SLA violations.
g) Penalties shall not exceed 100% of the monthly bill.
h) If the penalties exceed more than 50% of the total monthly bill, it will result in a material breach. In case of a material breach, the operator will be given a cure period of one month to rectify the breach failing which a notice to terminate may be issued by SAHRA.

10. EVALUATION CRITERIA

10.1. All proposal offers received shall be evaluated based on the following phase out approach:

- **Phase one**: Compliance to the terms of reference and conditions of the proposal. Failure to meet any of the conditions of the proposal will automatically disqualify your proposal on this phase.
- **Phase two**: Prequalification criteria (Obtaining the minimum threshold for functionality as set out below)

No.	Criteria	Weight
1.	Number of years providing cloud services. ➢ 1 year or less = **0** ➢ 1 to 3 years = 1 ➢ 4 to 6 years = **3** ➢ 7 to 9 years = **4** ➢ 10 years and above = **5**	**10**
2.	Physical Data Centre located in South African borders	**10**

	➢ No = 0 ➢ Yes = 5	
3.	Number of examples of government customers ➢ 0 – 1 example (Very Poor) = **1** ➢ 2 examples (Poor) = **2** ➢ 3 – 4 examples (Good) = **3** ➢ 5 examples (Very Good) = **4** ➢ 6 or more (Excellent) = **5**	**10**
4.	Quality of project proposal	**35**
5.	Quality of the Project Plan together with the Service level agreement	**10**
6.	Quality of the ICT security proposal and certification of the bidder e.g., ISO 27001, 27017 and 27018 certifications	**15**
	Total:	**90**
Phase 3: Presentations - Shortlisted service providers will be expected to present a short (no more than 10 minute) presentation that summarizes their proposal		
1.	Presentation	**10**

A bidder must obtain a minimum of 54 points out of 90 points on the prequalification phase (Phase 2) to progress to the next phase i.e., Phase 3 - Presentation. Failure to obtain 54 points will render your proposal nonresponsive.

A bidder must obtain a minimum of 6 points out of 10 points in phase Three (3) - Presentations to be considered for preference points.

- **Phase four**: preference points for Broad-Based Black Economic Empowerment (BBBEE) Status Level of Contribution (80/20 preference points system), where 80 points are allocated to price, and 20 points are allocated to BBBEE status level as follows.

B-BBEE Status Level of Contributor	Number of points (80/20 system)
1	20
2	18
3	14
4	12
5	8
6	6

7	4
8	2
Non-compliant contributor	0

10.2. Price (Vat included)

80 Points for price will be awarded with reference to the total fixed proposal amount inclusive of VAT. The service provider with the lowest price shall score the maximum 80 points.

11. REGISTRATION AND SUBMISSION OF CLARITY QUESTIONS

All bidders are required to register their interest by no later than 15:00 on 28 April 2021.

To register your interest please send the following information to Ms. Nancy Cloete (ncloete@sahra.org.za) by 15:00 on 28 April 2021.

1. Name of company
2. Name of contact person
3. Contact number.
4. Contact email.

Please include "Registration of Interest: Cloud Hosting RFP" in the subject line.

All registered bidders must submit any technical queries, in writing, to ncloete@sahra.org.za by 03 May 2021.

A written response to all queries will be sent to all registered bidders by C.O.B. on 07 May 2021.

12. SUBMISSION OF PROPOSALS

Bids must be submitted in a sealed envelope, marked as confidential and for the attention of
Supply Chain Management – Ms. Ayanda Fortunate Mkhize
Bid No: SAHRA/NIU/21/04/2021
Project Name: Provision of Cloud Services

BIDS must be placed in the Tender Box located at:
SAHRA's Head Office
111 Harrington Street,
Cape Town

SAHRA takes no responsibility for mailed tender documents. It is the onus of the service provider to ensure that the document is placed in the Tender Box before closing date and time.

13. ANTICIPATED TIME SCHEDULE AND PROCESS

Request for Tenders Issued	Website/ e-tender	21 April 2021
Registration of interest by bidders	Via email	28 April 2021
Submission of queries	Via email	03 May 2021
Response to Queries	Via email	07 May 2021
Closing date & Opening of BIDs	SAHRA Head Office	14 May 2021

14. FOR SUPPLY CHAIN RELATED ENQUIRIES, PLEASE CONTACT:

Ms. Ayanda Mkhize
Supply Chain Management
South African Heritage Resources Agency
111 Harrington Street
Cape Town
8000
Tel: 021 462 4502
Email: amkhize@sahra.org.za