Information and Communication Technology
Agency of Sri Lanka

BIDDING DOCUMENT

Addendum - 1

National Competitive Bidding (NCB)

Procurement of Service Provider for Support and Maintenance of Red Hat Open Stack Based Platform of Lanka Government Cloud (LGC 2.0)
[IFB No: ICTA/GOSL/SER/NCB/2023/05]

Information and Communication Technology Agency of Sri Lanka
490, R A de Mel Mawatha, Colombo 03.

May 2023

Accordingly Following documents are amended.

Section V

Schedule of Requirements

2. Scope of related services

2.1.1 Operations, support, and maintenance.

(6) Setting up and periodic reports and performance dashboards for the LGC 2.0(including not limited to ceph, openstack and rhev).

2. List of Related Services

2.1 Scope of Works:

2.1.1 Operations, support, and maintenance.

(1)	(2)	(3)	(4)
#	**Item**	**Compliance to the specification** (Yes / No) If "No" bidder's response	**Technical reference** (Please specify the page number)
1	The service provider should ensure the necessary infrastructure uptime and other SLAs. (Refer **the Annexure 01**) All the required updates/upgrades, patches, and security fixes released by the Product principle (Redhat) should be deployed and maintained in a timely manner.		
2	Continuous performance monitoring and tuning of the environment should be carried out.		
3	Scale up and scale-out among others Redhat Ceph underlying SDS ,Rhev, openstack Computes..etc when required.		
4	Further enhancements/upgrades/expansions have to be supported as and when required.		
5	Supportability assessments, early beta access, product life cycle planning, Support escalation and time attend reviews ... etc should be covered by Red Hat Principal's TAM (Technical Account Manager) for both Redhat OpenStack and Redhat Ceph.		
6	Setting up and maintenance periodic reports and performance dashboards for the LGC 2.0(including not limited to ceph, openstack and rhev, STF, ELK , Grafana ..etc relevant monitoring and alerting systems to be set up and maintained by bidder appropriately).		
7	24x7 industry-standard help-desk support with responsibility matrix. (Responsibility/ Escalation matrix should be provided by the bidder)		
8	Should perform an analysis on the alerts and incidents triggered in LGC 2.0 systems to detect the root cause of the incidents and fine-tune the configured rules. A detailed report including the action plan should be submitted to ICTA for necessary approval.		
9	Should maintain and operate secure access control matrix: Any access provisioning/de-provisioning/update should be reported within the defined timeline in the prescribed format and should be updated in the access control matrix/access list. The access list should be updated on a regular basis and the document should share with ICTA.		

(1)	(2)	(3)	(4)
10	Should prepare, maintain, and up to date all design/architecture documents, layouts, manuals, journals, standard operating procedures (SOP), and other supporting documents. Prior to finalizing should submit to ICTA to get confirmation (quarterly or when the document is updated).		
11	Performance Testing: Shall carry out Performance testing of the Compute/Storage/Network/ .etc solutions to ensure that it meets the performance requirements. (Every 6 months and when required)		
12	Fail over Testing: Shall carry out failover testing of the server/network/storage/. etc solutions to ensure that it meets the HA/redundancy requirements. (Every 6 months and when required)		
13	Shall maintain centralized logging capability (including events logs, security logs.etc) for audit, logs analysis & ease of management purposes (retention period should be a minimum of 3 months.		
14	Should maintain security logging and support integration with security solutions. Logs shall be time-stamped and shall include details like events and the activities performed, date and time stamps, terminal identity or location, user IDs, records of successful and rejected system access attempts, records of successful and rejected data, and other resource access attempts, etc.		
15	Periodically all device configurations, settings.etc should be backup (daily, weekly, and monthly basis)		
16	Shall require identifying parameters including, but not limited to, key resources in the storage solution, interconnects between key resources in the storage solution, the health of key resources, connectivity and access rights to storage volumes, and the zones being enforced in the storage solution.		
17	The Service Provider shall be responsible for real-time monitoring of all systems (one or minimum dashboards) and alerts should be configured to email. Sms (if possible)		
18	Preventive Maintenance (PM) should be carried out of all hardware and testing for viruses if any, and proper records should be maintained for such PM.		
19	Should adhere to the data protection ACT 9 of 2022 in all components.		
20	The service provider who engages with the assignment should sign an on-Disclosure Agreement (NDA) where applicable		
21	Training and Awareness: shall develop and implement plan/processes for training and awareness of ICTA nominate Engineers.		
22	Shall provision skilled and experienced manpower resources to administer, Operations, and manage the entire solution. Manpower should consist of at least Architect, Tech lead		

(1)	(2)	(3)	(4)
	relevant domains engineers(eg – Openstack,ceph,rhev..etc engineers), Project Manager/Account Manager).		
23	Shall be responsible for identification, diagnosis, and resolution of problem areas pertaining to the IT Infrastructure (LGC2.0) and maintaining the defined SLA levels.		
24	Periodic Reporting of Service Levels a) Reporting of risks and issues with mitigation strategies to the Immediate action to mitigate the identified risks and issues. b) The Service Levels and performance measurement reports should be submitted in an agreed-upon format (Monthly Report). c) The bidder should submit monthly reports. Monthly Service report should include: Health check report, Resource utilization report, Incidents and RCA reports.		

2.2 Data Privacy, Security and Data Protection:

2.2.1 Data Privacy and Security:

#	**Item**	**Compliance to the specification** (Yes / No) If "No" bidder's response	**Technical reference** (Please specify the page number)
1	Service provider should be responsible for all aspects of data privacy		
2	Need to follow best security practices and ensure safe and sound confidentiality and availability		

2.3 Data Protection:

2.3.1 Service provider will be compliant with the following specific data protection principles.

#	**Item**	**Compliance to the specification** (Yes / No) If "No" bidder's response	**Technical reference** (Please specify the page number)
1	Respect of data quality principles		
2	Requirements with regard to any data transfers outside		
3	Audits		
4	Back-ups, logs and audit trails		
5	Personal data breaches		
6	Data portability		