Anx-Vol-2.6

Cloud services and related Functional requirement

1.0 Cloud services as a Control Centre/ Central Computer System

1. Cloud based Services Requirement / Specifications

The **bidder** should provide the public/private cloud based services includes IaaS, PaaS, SaaS services. The Cloud-computing platform must be ISO27001:2005 or higher, DATA Centre must be III tier + and third-party vulnerability certifications comprise the following functional requirements:

I. World-Class Security – Provision of world-class security at every level.
II. Trust and Transparency – Provide transparent, real-time, accurate service performance and availability information.
III. True Multi-tenancy – Deliver maximum scalability and performance with a true multitenant architecture.
IV. Proven Scale – Support millions of users with proven scalability.
V. High Performance – Deliver consistent, high-speed performance globally as per Standards.
VI. Complete Disaster Recovery – Protect data by running the service on multiple, geographically dispersed data centres with extensive backup, data archive, and failover capabilities.
VII. High Availability – Equip world- Corporate class facilities with proven high-availability infrastructure and application software.

2. World-Class Security

Provision of world-class security at every level.

Security is more than just user privileges and password policies. It's a multidimensional business imperative, especially for platforms that are responsible for utility data. Cloudcomputing platform must have detailed, robust policies and procedures in place to guarantee the highest possible levels of:

I. Physical security
II. Network security
III. Application security
IV. Internal systems security
V. Secure data-backup strategy
VI. Secure internal policies and procedures
VII. Third-party certification

3. Trust and Transparency

Functional Requirements

Provision of transparent, real-time, accurate service performance and availability information.

Cloud-computing platform should provide utility with detailed information about service delivery and performance in real time, including:

I. Accurate, timely, and detailed information about service performance data and planned maintenance activities
II. Daily data on service availability and transaction performance
III. Proactive communications regarding maintenance activities

4. True Multi-tenancy

Deliver maximum scalability and performance with a true multitenant architecture.

Multi-tenancy should be provided to utility with the following benefits:

I. Efficient service delivery, with a low maintenance and upgrade burden
II. Consistent performance and reliability based on an efficient, large-scale architecture
III. Rapid product release cycles

5. Proven Scale

Support millions of users with proven scalability.

With cloud-computing service, utility should be benefited from the scale of the platform. A larger scale means a larger user community, which can deliver more and higher-quality feedback to drive future platform innovation. A larger user community also provides rich opportunities for collaboration between users, creating communities that can share interests and foster best practices. Cloud-computing platform must have:

I. Proof of the ability to scale to hundreds of thousands of subscribers/ users
II. Resources to guarantee the highest standards of service quality, performance, and security to every user
III. The ability to grow systems and infrastructure to meet changing demands
IV. Support that responds quickly and accurately to every user
V. Proven performance and reliability as user numbers grow

6. High Performance

Deliver consistent, high-speed performance globally.

Cloud-computing platforms must deliver consistent, high-speed systems performance worldwide and provide detailed historical statistics to back up performance claims, including:

I. Average page response times
II. Average number of transactions per day

7. Complete Disaster Recovery

Protect user data by running the service on multiple, geographically dispersed data centers with extensive backup, data archive, and failover capabilities.

Platforms providing cloud-computing services must be flexible enough to account for every potential disaster. A complete disaster recovery plan includes:

I. Data backup procedures that create multiple backup copies of users' data, in near real time, at the disk level

II. A multilevel backup strategy that includes disk-to-disk-to-tape data backup in which tape backups serve as a secondary level of backup, not as the primary disaster-recovery data source. This disk-oriented model ensures maximum recovery speed with a minimum potential for data loss in the event of a disaster.

8. High Availability

Equip world-class facilities with proven high availability infrastructure and application software.

Any platform offering cloud-computing applications needs to be able to deliver very high availability.

Requirements for proving high availability include:

I. Facilities with reliable power, cooling, and network infrastructure

II. High-availability infrastructure: networking, server infrastructure, and software

III. N+1 redundancy

IV. Detailed historical availability data on the entire service, not just on individual servers

2.0 Network Data Security

The following items need to be considered for adequate security at different levels i.e. systems, data, network and security and Project implementing consortium needs to provide

Systematic description of how data security is maintained from the meters to the system head end. All elements of the proposed system shall support protection of data, confidentiality, data integrity and operational security. Physical security to prevent on-site tampering to be ensured.

1. System should enable creation and maintenance of accounts, passwords and functionality access levels, along with log details.
2. Description of the in-built anti-virus capabilities provided in connection with all proposed software platforms and solutions.
3. Description of methods to detect and prevent attacks including but not limited

1. Access Control

There shall be an identity and access management system which shall control and log the access control of all users to the smart grid systems.

1. The identity and access management system shall be able to define the access control levels of each user based on roles, responsibilities or hierarchy.

Functional Requirements

2. The identity and access management system shall be able to define which user can access which function of the individual systems. For example, the identity and access management system shall define which user can initiate a load disconnect function for a particular consumer, and therefore rest of the unauthorized users will not be able to perform load disconnect function.
3. The identity and access management system shall be integrated with rest of the Centralized Computer Systems.

3.0 Network Security

1. Since Centralized Computer System has to access external environment through GPRS and Internet cloud it is important to have adequate network security systems.
2. There shall be intrusion detection and prevention systems deployed at the central layer.
3. There shall also be firewalls which will be a separate system from the intrusion prevention system.
4. The firewall shall control the demilitarized zones in the data centre and control room, and also the systems and ports which will be open to public network/ VPN.
5. If fixed IP and operator VPN is not available / possible and Dynamic IP is being used, then the devices shall support SSL/VPN and the data shall be encrypted before send / received on GPRS/CDMA last mile network, for devices consisting of Smart Meter Network SMN.

4.0 System and Data security

1. The systems deployed shall have the application scanning, hardware scanning tools in order to identify any vulnerability so as to mitigate any potential security threats.
2. The application databases shall have exclusive security tools in order to prevent any potential internal attacks like SQL injection etc.
3. The data shall be encrypted wherever supported by existing systems/devices/technology.

5.0 Billing system

GUVNL already having a billing system in place. The details of the Billing System is as below:

A billing system capable of handling the billing of time based rates and existing employer billing rate will be required to be deployed. Project implementing consortium shall describe the billing system integration with the existing billing system. System should have facility to make billing based on slot wise energy, frequency and UI mechanism, peak time/ off peak time/ rest hrs etc. Necessary billing parameters should be transferred to existing billing application to prepare timely and accurate bills of consumers.

6.0 Service Level Agreements

1. The purpose of this Service Level Requirements/Agreement (hereinafter referred to as SLA) is to clearly define the levels of service which shall be provided by the Bidder to **GUVNL** for the duration of this contract period of the Project.
2. Timelines specified in the above section (Work Completion Timelines and Payment Terms) shall form the Service Levels for delivery of Services specified there-in.
3. All the payments to the Bidder are linked to the compliance with the SLA metrics specified in this document.

4. The SLA are proposed to be performance based. For purposes of SLA, the definitions and terms as specified along with the following terms shall have the meanings set forth below:

   a. "Uptime" shall mean the time period for which the IT Infrastructure Solution along with specified services / components with specified technical and service standards are available for users in all in-scope Applications across the GUVNL application landscape. Uptime, in percentage, of any component (Non IT and IT) can be calculated as : Uptime = {1- [(System Downtime) / (Total Time – Planned Maintenance Time)]} * 100

   b. "Downtime" shall mean the time period for which the IT Infrastructure Solution and/or specified services / components with specified technical and service standards are not available to users. This includes Servers, Routers, Firewall, Switches, all servers and any other IT and non-IT infrastructure, their subcomponents etc. at all Project locations etc. The planned maintenance time / scheduled downtime will include activities like software upgrades, patch management, security software installations etc.

   c. The selected Bidder will be required to schedule 'planned maintenance time' with prior approval of GUVNL. This will be planned outside working time. In exceptional circumstances, GUVNL may allow the MSP to plan scheduled downtime in the working hours.

   d. "Incident" refers to any event / abnormalities in the functioning of the IT

Infrastructure solution and services that may lead to disruption in normal operations.

   e. "Resolution Time" shall mean the time taken (after the incident has been reported at the helpdesk), in resolving (diagnosing, troubleshooting and fixing) or escalating (to the second level) getting the confirmatory details about the same from the bidder and conveying the same to the end user), the services related troubles during the first level escalation.

Commencement of SLA: The SLA shall commence from implementation period itself for adherence to the implementation plan. The penalty will be deducted from the next payment milestone during the implementation period. During the O & M period, the penalty will be deducted from the quarterly payments.

Sr. No	Parameter	Target	Basis	Penalty
Cloud Services related				
1	Provisioning and Deprovisioning of Virtual Machines	Within 15 minutes	Per occurrence. This will be calculated monthly	a) Within 15 minutes - Nil b) >15 minutes & <=45 min - 5% of the QP c) Beyond 45 minutes, for every 30 minutes of delay - 5% of QP
2	Overall Cloud Solution Availability	>= 99.95%	Per occurrence. This will be calculated monthly	a) <99.95% to >= 99.90% - 10% of QP b) <99.90% to >= 99.75% - 15% of QP c) <99.75% to >= 99.25% - 20% of QP d) Subsequently, for every 0.5% drop in SLA criteria - 10% of QP
3	Cloud Network Availability	>= 99.95%	Per occurrence. This will be calculated monthly	a) <99.95% to >= 99.90% - 10% of QP b) <99.90% to >= 99.75% - 15% of QP c) <99.75% to >= 99.25% - 20% of QP d) Subsequently, for every 0.5% drop in SLA criteria - 10% of QP

4	Cloud Virtualization Layer Availability	>= 99.95%	Per occurrence. This will be calculated monthly	a) <99.95% to >= 99.90% - 10% of QP b) <99.90% to >= 99.75% - 15% of QP c) <99.75% to >= 99.25% - 20% of QP d) Subsequently, for every 0.5% drop in SLA criteria - 10% of QP
5	Cloud Storage Availability	>= 99.95%	Per occurrence. This will be calculated monthly	a) <99.95% to >= 99.90% - 10% of QP b) <99.90% to >= 99.75% - 15% of QP c) <99.75% to >= 99.25% - 20% of QP d) Subsequently, for every 0.5% drop in SLA criteria - 10% of QP
6	Virtual Operating System Availability	>= 99.95%	Per occurrence. This will be calculated monthly	a) <99.95% to >= 99.90% - 10% of QP b) <99.90% to >= 99.75% - 15% of QP c) <99.75% to >= 99.25% - 20% of QP d) Subsequently, for every 0.5% drop in SLA criteria - 10% of QP
Sr. No	**Parameter**	**Target**	**Basis**	**Penalty**
7	Cloud Orchestration layer availability	>= 99.95%	Per occurrence. This will be calculated monthly	a) <99.95% to >= 99.90% - 10% of QP b) <99.90% to >= 99.75% - 15% of QP c) <99.75% to >= 99.25% - 20% of QP d) Subsequently, for every 0.5%

				drop in SLA criteria - 10% of QP
8	Cloud Security Layer Availability	>= 99.95%	Per occurrence. This will be calculated monthly	a) <99.95% to >= 99.90% - 10% of QP b) <99.90% to >= 99.75% - 15% of QP c) <99.75% to >= 99.25% - 20% of QP d) Subsequently, for every 0.5% drop in SLA criteria - 10% of QP

Note:

1. The MSP has to submit all the reports pertaining to SLA Review process within 7 working days after end of the quarter.
2. All the reports must be made available to GUVNL, as and when the report is generated or as and when asked by the competent authority.
3. In case the issue is still unresolved, the arbitration procedures described in the Terms & Conditions section will be applicable.
4. The down time will be calculated on monthly basis. Non-adherence to any of the services as mentioned below will lead to penalty as per the SLA clause and will be used to calculate downtime. The downtime calculated shall not include the following
    a. Down time due to hardware/software and application which is owned by GUVNL at their premises
    b. Negligence or other conduct of GUVNL or its agents, including a failure or malfunction resulting from applications or services provided by GUVNL or its vendors.

c. Failure or malfunction of any equipment or services not provided by the MSP.

5. However, it is the responsibility/ onus of the selected Bidder to prove that the outage is attributable to GUVNL. The selected Bidder shall obtain the proof authenticated by the GUVNL's official that the outage is attributable to the GUVNL.
6. The total deduction per quarter shall not exceed 20% of the total QP value
7. Two consecutive quarterly deductions amounting to more than 20% of the QPs on account of any reasons will be deemed to be an event of default and termination
8. It is the right of the GUVNL to bring/deploy any external resources / agencies at any time for SLA review
9. No Carry forward of any penalties of SLA calculations can be done from any of the preceding quarters

The Agency shall deploy sufficient manpower suitably qualified and experienced in shifts to meet the SLA. Agency shall appoint as many team members as deemed fit by them, to meet the time Schedule and SLA requirements.