<u>**Annexure – A 2.2.1**</u>

Cloud services (Data Centre) and related Functional requirement

Cloud services as a Control Centre/ Central Computer System

1. Cloud based Services Requirement / Specifications

The integrator 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 II tier + and third-party vulnerability certifications comprise the following functional requirements:

1. World-Class Security – Provision of world-class security at every level.
2. Trust and Transparency – Provide transparent, real-time, accurate service performance and availability information.
3. True Multi-tenancy – Deliver maximum scalability and performance with a true multitenant architecture.
4. Proven Scale – Support millions of users with proven scalability.
5. High Performance – Deliver consistent, high-speed performance globally as per Standards.
6. Complete Disaster Recovery – Protect data by running the service on multiple, geographically dispersed data centres with extensive backup, data archive, and failover capabilities.
7. 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. Cloud-computing platform must have detailed, robust policies and procedures in place to guarantee the highest possible levels of:

- Physical security
- Network security
- Application security
- Internal systems security
- Secure data-backup strategy
- Secure internal policies and procedures
- Third-party certification like certinetc approved by Government of India

3. Trust and Transparency

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:

- Accurate, timely, and detailed information about service performance data and planned maintenance activities
- Daily data on service availability and transaction performance
- 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:

- Efficient service delivery, with a low maintenance and upgrade burden
- Consistent performance and reliability based on an efficient, large-scale architecture
- 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:

- Proof of the ability to scale to hundreds of thousands of subscribers/ users
- Resources to guarantee the highest standards of service quality, performance, and security to every user
- The ability to grow systems and infrastructure to meet changing demands
- Support that responds quickly and accurately to every user
- 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:

- Average page response times

- 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:

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

- Facilities with reliable power, cooling, and network infrastructure
- High-availability infrastructure: networking, server infrastructure, and software
- N+1 redundancy
- Detailed historical availability data on the entire service, not just on individual servers

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

Access Control

1. 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.
2. The identity and access management system shall be able to define the access control levels of each user based on roles, responsibilities or hierarchy.
3. 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.
4. The identity and access management system shall be integrated with rest of the Centralized Computer Systems.

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.

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.