Corrigendum-I to the Tender No: 511532

S.No	Clause	Query raised	May be read as
1	4 (1)	Can the EMD of Rs 1,00,000/- mentioned in the RFP be waived for MSME participants	EMD will be waived off for MSME
2	ANNEXURE 5	Should the pricing be given for DR site in the Financial proposal as it is mentioned in Technical proposal and not in the Financial proposal	Bidder has to submit combined pricing for DC + DR .DR site is to be maintained which comprises of Web and DB Server in single VM. Indicative Hosting requirements for DR are at Annexure A
		DR site to be maintained which comprises of Web and DB Server in single VM	
3		Contract period is not mentioned	Contract period will be for one year and further extension will be decided based on performance
4	3 (6)	SLA is not mentioned	Document attached at Annexure B.
5		Security requirement not mentioned - Firewall and its management	Document attached at Annexure C.
6	5	Requested for extension of time	Pre bid meeting 02/04/2024 at 03:00 PM Bid closing date 04/04/2024 Bid opening date 05/04/2024.

Annexure A
Indicative Hosting requirements for DR

	OS	CPU	RAM	Storage	Units
Web Server + Database Server (DB-PostGreSQL)	RHEL	vCore – 8	64 GB	500 GB	1

Annexure B
Service Level Agreement

1. Service Level Agreement

Meity has announced MeghRaj Policy to provide strategic direction for adoption of cloud services by the Government (http://meity.gov.in/content/gi-cloud-initiative-meghraj). The aim of the cloud policy is to realize a comprehensive vision of a government cloud (GI Cloud) environment available for use by central and state government line departments, districts and municipalities to accelerate their ICT - enabled service improvements. MeghRaj policy of Meity states that "Government departments at the Centre and States to first evaluate the option of using the GI Cloud for implementation of all new projects funded by the government. Existing applications, services and projects may be evaluated to assess whether they should migrate to the GI Cloud."

1.1 Purpose

- The purpose of Service Levels is to define the levels of service provided by the Cloud Service Provider ("CSP") to Telangana State Electricity Regulatory Commission ("Client") for the duration of the contract. The benefits of this are:
  - o Help the Client control the levels and performance of CSP's services.
  - o Create clear requirements for measurement of the performance of the system and help in monitoring the same during the Contract duration.
- The Service Levels are between the Client and CSP.

1.2 Service Level Agreements & Targets

- This section is agreed to by Client and CSP as the key performance indicator for the project.
- The following section reflects the measurements to be used to track and report system's performance on a regular basis. The targets shown in the following tables are for the period of Contact.

1.3 General Principles of Service Level Agreements

Service Level Agreement (SLA) shall become the part of the Contract between the Client and the CSP. SLA defines the terms of CSP's responsibility in ensuring the timely delivery of the services and the correctness of the services based on the agreed performance indicators as detailed in this section.

The CSP shall comply with the SLAs to ensure adherence to project quality and availability of services throughout the duration of the Contract. For the purpose of the SLA, definitions and terms as specified in the document along with the following terms shall have the meanings set forth below:

“Total Time” – Total number of hours in the quarter being considered for evaluation of SLA performance.

“Downtime” – Time period for which the specified services/components/system are not available in the concerned period, being considered for evaluation of SLA, which shall exclude downtime owing to Force Majeure and reasons beyond control of the CSP.

“Scheduled Maintenance Time”– Time period for which the specified services/components/system with specified technical and service standards are not available due to scheduled maintenance activity. The CSP shall seek at least 15 days’ prior written approval from the Client for any such activity. The scheduled maintenance shall be carried out during non-peak hours and shall not exceed more than four (4) hours and not more than four (4) times in a year.

“Uptime” – Time period for which the specified services are available in the period being considered for evaluation of SLA.

Uptime (%) = (1- {[Total Downtime] / [Total Time- Scheduled Maintenance Time]}) * 100. Penalties shall be applied for each criterion individually and then added together for the total penalty for a particular quarter

“Incident” – Any event/abnormalities in the service/system being provided that may lead to disruption in regular/normal operations and services to the end user.

“Response Time” – Time elapsed from the moment an incident is reported to the Helpdesk either manually or automatically through the system to the time when a resource is assigned for the resolution of the same.

“Resolution Time” – Time elapsed from the moment incident is reported to the Helpdesk either manually or automatically through system, to the time by which the incident is resolved completely and services as per the Contract are restored.

“Target” – is the availability of cloud and managed services and their data. It is calculated as = [(Total uptime of all cloud and managed services in a quarter)/(Total time in quarter)]*100.

Latency: Latency may address the storage and the time when the data is placed on mirrored storage. Maximum Data Restoration Time: refers to the committed time taken to restore cloud service customer data from a backup.

Recovery Point Objective: It is the maximum allowable time between recovery points. RPO does not specify the amount of acceptable data loss, only the acceptable time window. RPO affects data redundancy and backup.

Recovery Time Objective: It is the maximum amount of time a business process may be disrupted, after a disaster, without suffering unacceptable business consequences. Cloud services can be critical components of business processes.

Availability of Reports (Reports such as Provisioning, Utilization Monitoring Reports, User Profile Management etc.)

Penalty shall be applied for each criterion individually as per downtime of each applicable component and then added together for the total penalty for a particular quarter.

1.4 Service Levels Monitoring

- The Service Level parameters shall be monitored on a quarterly basis. Penalties associated with performance for SLAs shall be made after deducting from applicable payments of the quarter or through the Performance Bank Guarantee.
- As part of the Project requirements, CSP shall supply and make sure of appropriate system (software/hardware) to automate the procedure of monitoring SLAs during the course of the Contract and submit reports for all SLAs as mentioned in this section. This software along with any system specific software shall be used by the CSP for monitoring and reporting these SLAs. The Client reserves the right to test and audit these tools for accuracy and reliability at any time. If at any time during the test and audit the accuracy and reliability of tools shall be found to be compromised, the Client reserves the right to invoke up to double the penalty of the respective quarterly phase.
- The CSP will endeavour to exceed these levels of service wherever possible.
- CSP undertakes to notify the Client of any difficulties, or detrimental/adverse findings as soon as possible once they are identified.
- CSP will provide a supplemental report on any further information received, as soon as the information becomes available.
- CSP will take instruction only from authorized personnel of the Client.
- In case issues are not rectified to the complete satisfaction of Client, within a reasonable period of time defined in the RFP, the Client shall have the right to take appropriate remedial actions including liquidated damages, applicable penalties, or termination of the Contract.
- For issues i.e. breach of SLAs beyond control of the CSP, the CSP shall submit a justification for the consideration of the Client. In case it is established that the CSP was responsible for such breach, respective penalty shall be applied to the CSP.

1.5 Measurements & Targets - Operations Phase SLAs

- These SLAs shall be used to evaluate the performance of the services post the Implementation Phase and during the operations Phase. These SLAs and associated performance shall be monitored on a quarterly basis. Penalty levied for non-performance as per SLA shall be deducted through subsequent payments due from the Client or through the Performance Bank Guarantee.
- The Scheduled Maintenance Time shall be agreed upon with the Client as per the definition given as part of this section of the Contract.
- CSP's published SLAs and penalties shall be also being applicable during the course of the Contract.
- While the CSP will be responsible for maintaining the SLAs pertaining to the cloud infrastructure, network, controls etc., the MSP will be responsible for the SLAs related to managing and monitoring the cloud services.

S.No	Service Level	Measurement	Target/Service	Penalty (Indicative)
	Objective	Methodology	Level	
Availability/Uptime				
1	Availability/Uptime of cloud services Resources for Production environment (VMs, Storage, OS, VLB, Security Components,)	Availability (as per the definition in the SLA) will be measured for each of the underlying components (e.g., VM, Storage, OS, VLB, Security Components) provisioned in the cloud.	Availability for each of the provisioned resources: >=99.5%	Default on any one or more of the provisioned resource will attract penalty as indicated below. =<99.5% - >=99% (10% of the <MP>) < 99% (30% of the (MP)
2	Availability of Critical Services (e.g., Register Support Request or Incident; Provisioning / De-Provisioning; User Activation / Deactivation; User Profile Management; Access Utilization Monitoring Reports) over User / Admin Portal and APIs (where applicable)	Availability (as per the definition in the SLA) will be measured for each of the critical services over both the User / Admin Portal and APIs (where applicable)	Availability for each of the critical services over both the User / Admin Portal and APIs (where applicable) >= 99.5%	Default on any one or more of the services on either of the portal or APIs will attract penalty as indicated below. =<99.5% - >=99% (10% of the <MP>) < 99% (20% of the <MP>)
3	Availability of the network links at DC and DR (links at DC / DRC, DCDRC link)	Availability (as per the definition in the SLA) will be measured for each of the network links provisioned in the cloud.	Availability for each of the network links: >= 99.5%	Default on any one or more of the provisioned network links will attract penalty as indicated below. =<99.5% - >=99% (10% of the <MP>)
4	Availability of Regular Reports (e.g., Audit, Certifications,) indicating the compliance to the Provisional empanelment Requirements.		15 working days from the end of the quarter. If STQC issues a certificate based on the audit then	5% of MP

S.No	Service Level	Measurement	Target/Service	Penalty (Indicative)
	Objective	Methodology	Level	
			this SLA is not required.	
Support Channels - Incident and Helpdesk				
5	Response Time	Average Time taken to acknowledge and respond, once a ticket/incident is logged through one of the agreed channels. This is calculated for all tickets/incidents reported within the reporting month	95% within 15minutes	<95% & >=90% (5% of the MP) < 90% & >= 85% (7% of the MP) < 85% & >= 80% (9% of the MP)
6	Time to Resolve - Severity 1	Time taken to resolve the reported ticket/incident from the time of logging.	For Severity 1, 98% of the incidents should be resolved within 30 minutes of problem reporting	<98% & >=90% (5% of the MP) < 90% & >= 85% (10% of the MP) < 85% & >= 80% (20% of the MP)
7	Time to Resolve - Severity 2,3	Time taken to resolve the reported ticket/incident from the time of logging.	95% of Severity 2 within 4 hours of problem reporting & 95% of Severity 3 within 16 hours of problem reporting	<95% & >=90% (2% of the MP) < 90% & >= 85% (4% of the MP) < 85% & >= 80% (6% of the MP)
Security Incident and Management Reporting				
8	Percentage of timely incident report	Measured as a percentage by the number of defined incidents reported within a predefined time (1 hour) limit after discovery, over the total number of defined incidents to the cloud service which are reported within a predefined period (i.e. month). Incident Response - CSP shall assess and acknowledge the defined incidents within 1 hour after discovery.	95% within 1 hour	<95% & >=90% (5% of the MP) < 90% & >= 85% (10% of the MP) < 85% & >= 80% (15% of the MP)

S.No	Service Level	Measurement	Target/Service	Penalty (Indicative)
	Objective	Methodology	Level	
9	Percentage of timely incident resolutions	Measured as a percentage of defined incidents against the cloud service that are resolved within a predefined time limit (month) over the total number of defined incidents to the cloud service within a predefined period. (Month). Measured from Incident Reports	95% to be resolved within 1 hour	<95% & >=90% (5% of the MP) < 90% & >= 85% (10% of the MP) < 85% & >= 80% (15% of the MP)
Vulnerability Management				
10	Percentage of timely vulnerability corrections	The number of vulnerability corrections performed by the cloud service provider - Measured as a percentage by the number of vulnerability corrections performed within a predefined time limit, over the total number of vulnerability corrections to the cloud service which are reported within a predefined period (i.e. month, week, year, etc.). • High Severity Vulnerabilities – 30 days - Maintain 99.95% service level • Medium Severity Vulnerabilities – 90 days - Maintain 99.95% service level	99.95%	>=99% & <99.95% (10% of the MP) >=98% & <99% (20% of the MP) <98% (30% of the MP)
11	Percentage of timely vulnerability reports	Measured as a percentage by the number of vulnerability reports within a predefined time limit, over the total number of vulnerability reports to the cloud service which are reported within a predefined period (i.e. month, week, year, etc.).	99.95%	>=99% & <99.95% (10% of the MP) >=98% & <99% (20% of the MP) <98% (30% of the MP)
Vulnerability Management				

S.No	Service Level	Measurement	Target/Service	Penalty (Indicative)
	Objective	Methodology	Level	
12	Security breach including Data Theft/Loss/Corruption	Any incident where in system compromised or any case wherein data theft occurs (including internal incidents)	No breach	For each breach/data theft, penalty will be levied as per following criteria. Any security incident detected INR << 5 Lakhs>>.This penalty is applicable per incident. These penalties will not be part of overall SLA penalties cap per month. In case of serious breach of security wherein the data is stolen or corrupted, << Government Department / Agency>> reserves the right to terminate the contract
13	Availability of SLA reports covering all parameters required for SLA monitoring within the defined time		(e.g., 3 working days from the end of the month)	5% of MP
Service levels DR				
14	Recovery Time Objective (RTO) (Applicable when taking Disaster Recovery as a Service from the Service Provider)	Measured during the regular planned or unplanned (outage) changeover from DC to DR or vice versa.	<<= 4 hours>> [Government Department / Agency to indicate based on the application requirements]	10% of MP per every additional 4 (four) hours of downtime
15	Recovery Point Objective (RPO) (Applicable when taking Disaster Recovery as a Service from the Service Provider)	Measured during the regular planned or unplanned (outage) changeover from DC to DR or vice versa.	<= 2 hours [Government Department / Agency to indicate based on the application requirements]	10% of MP per every additional 2 (four) hours of downtime
16	Availability of Root Cause Analysis (RCA) reports for Severity 1 & 2		Average within 5 Working days	5% of MP

Note: MP means Monthly Payment

1.6 Severity Level

Below severity definition provide scenarios for incidents severity.

Severity Level	Description	Example
Severity 1	Environment is down or major malfunction resulting in an inoperative condition or disrupts critical business functions and requires immediate attention. A significant number of end users (includes public users) are unable to reasonably perform their normal activities as essential functions and critical programs are either not working or are not available	Non-availability of VM. No access to Storage, software, or application
Severity 2	Loss of performance resulting in users (includes public users) being unable to perform their normal activities as essential functions and critical programs are partially available or severely restricted. Inconvenient workaround or no workaround exists. The environment is usable but severely limited.	Intermittent network connectivity
Severity 3	Moderate loss of performance resulting in multiple users (includes public users) impacted in their normal functions.	

Annexure C
Security Requirements

VMs should be firewall protected. The network architecture must be secure with support for Firewall and encryption. The system shall also allow host-based firewalls to be configured, as an additional layer of security if the network firewall were to fail.

The CSP should ensure complete security requirements for the Government Community Cloud hosting of department with suitable security arrangements through SaaS model (Security as a Service) as per Meity guidelines. CSP shall provide end-to-end security services to meet IT security challenges for the Infrastructure based on the proven frameworks and security best practices. It is vital for complete security that the processes and technology which shall support the Information Security function are proven and adhere to standards.

It is envisaged that the security operations shall be centralized, structured and coordinated and shall be responsive resulting in effective threat prevention and detection helping the deployed cloud solution to be secure from attackers. The Information Security functions shall respond faster, work collaboratively, and share knowledge more effectively. The proposed cloud solution shall have multiple security layers to secure the infrastructure from threats. CSP shall propose and provide security solutions that may not be mentioned in the RFP but are required as per the guidelines of Meity.

CSP shall provision for following security solutions (not limited to):

- Next-Generation Firewall (NGFW) having minimum 2Gbps threat-prevention throughput (all features enabled).

- Web Application Firewall for OWASP Top 10 protection

- IPS/IDS

- HIPS

- Malware Analysis - CSP shall conduct analysis of newly discovered malware to uncover its scope and origin.

- DDoS service - CSP would offer DDOS Protection to protect the cloud infrastructure and application from well-equipped attackers. Minimum mitigation of 1 Gbps.

- Anti-Virus - This Service includes virus detection and eradication, logon administration and synchronization across servers, and support for required security classifications.

- SIEM - The CSP shall also propose for Security Information and Event Management (SIEM) solution supporting threat detection and security incident response through the real-time collection and historical analysis and correlation of security events from a wide variety of event and contextual data sources. It shall also support compliance reporting and incident investigation through analysis of historical data from these sources.

• VAPT – The CSP shall conduct vulnerability and penetration test (from a third-party testing agency which has to be CERT-IN empaneled) on the Cloud facility every 6 months and reports shall be shared with department. The CSP needs to update the system in response to any adverse findings in the report, without any additional cost to department.

• Security solution during data in transit and at rest

It is critical to have a set of IT security management processes and tools to ensure complete security of cloud solution. An IT security policy, framework and operational guidelines as per ISO 27001, 27017, 27018 & PCI-DSS be maintained & implemented by Cloud service provider (CSP).

Department will perform physical audits and will require access as and when required by department.

All the security management processes, tools and usage shall be well documented in security policy and the security best practices to be followed to maintain IT security.

Data shall not leave the Indian boundaries and data residing within Cloud shall not be accessed by any entity outside the control of department.

Cloud service shall support audit features such as what request was made, possibly the source IP address from which the request was made, who made the request, when it was made, and so on.

Security Controls

CSP shall provide adequate security controls not limited to the measures as described below:

• Secure Access Controls

o The system shall include mechanisms for defining and controlling user access to the operating system environment and applications. Best practices from enterprise security including password strength, password aging, password history, reuse prevention etc. must be followed for access control.

• Authorization Controls

o A least-privilege concept such that users are only allowed to use or access functions for which they have been given authorization shall be available.

• Logging

o Logs must be maintained for all attempts to log on (both successful and unsuccessful), any privilege change requests (both successful and unsuccessful), user actions affecting security (such as password changes), attempts to perform actions not authorized by the authorization controls, all configuration changes etc. Additionally,

the access to such logs must be controlled in accordance to the least privilege concept mentioned above, so that entries may not be deleted, accidentally or maliciously.

• Hardening

o All unnecessary packages must be removed and/or disabled from the system. Additionally, all unused operating system services and unused networking ports must be disabled or blocked. Only secure maintenance access shall be permitted and all known insecure protocols shall be disabled.

• Malicious Software Prevention

o Implementation of anti-virus software and other malicious software prevention tools shall be supported for all applications, servers, data bases etc.

• Network Security

o The network architecture must be secure with support for UTM, Firewall and encryption. The system shall also allow host-based firewalls to be configured, as an additional layer of security if the network firewall were to fail.

o Cloud services shall be provided on a scalable network connectivity between the server and Storage and Network. Cloud service shall be able to support multiple (primary and additional) network interfaces. The proposed data center shall be isolated from failures in other data centers. CSP proposed data center shall be connected with low latency and in-expensive network connectivity.

Cloud service provider should able to configured the secure network over an internet like IPsec VPN tunnel or SSL VPN.

o Cloud services shall provide a web interface with support for multi-factor authentication to access and manage the resources deployed in cloud and also provide Audit Trail of the account activity to enable security analysis, resource change tracking, and compliance auditing.

• Information Security: Log Monitoring and Correlation

o All Servers / sub systems / network devices / appliances as proposed shall have capability and throw logs to the log server. The Logs and events generated by VMs, applications, DB, network, security component / devices of the system shall be monitored. CSP must provide a Security information and event management (SIEM) solution for the same which shall be capable to provide various security alerts, events,logs generated from various IT infrastructure (Hardware/Software) components. CSP would need to ensure the IT security compliance and therefore monitor the threats/logs generated by various equipment's / sub systems.