Service Level Agreement And Packages

WEB APPLICATION FIREWALL

MeitY Empanelled Basic Cloud Service

PREAMBLE: MeitY Empanelled Basic Cloud Service contracts placed through GeM shall be governed by following set of Terms and Conditions:

1. General terms and conditions for Goods and Services;
2. Service Specific STC of MeitY Empanelled Basic Cloud Service – as defined in Service Catalogue which includes SLA for the Service or Service for a particular product;
3. BID / Reverse Auction specific ATC
4. Operation of The above terms and conditions are in reverse order of precedence i.e. ATC supplement Service Specific STC and GTC, however, Service Specific STC prevails or supersede over the GTC.
5. The above set of conditions along with Scope of supply including price as enumerated in the Contract Document shall be construed to be part of the contract.
6. This document represents a comprehensive Terms and Conditions governing the contract between the Buyer and Service Provider. The purpose of this document is to outline the scope of work, Stakeholder's obligation and terms and conditions of all services covered as mutually understood by the stakeholder

Agreement Overview

This Agreement represents a Service Level Agreement ("SLA" or "Agreement") between the buyer and Cloud Services provider.

The purpose of this agreement is to facilitate the implementation of Cloud Measures at the buyer's premises. The service provider would provide the required equipment and personnel for the mentioned services as per the requirements of the buyer.

This Agreement outlines the scope of work, Stakeholder's obligation and general terms and conditions of all services covered as they are mutually understood by the stakeholders.

The Agreement remains valid until superseded by a revised agreement mutually endorsed by the stakeholders.

1.1

Th ders associated with this SLA are:

1) Service Provider(s)

2) Buyer

3) Paying Authority

4) Statutory/Compliance Authority

The responsibilities and obligations of the stakeholders have been outlined in this document. The document also encompasses payment terms and penalties in case of non-adherence to the defined terms and conditions. It is assumed that all stakeholders would have read and understood the same before signing the SLA.

Objective and Goals

The objective of this Agreement is to ensure that the proper elements and commitments are in place to provide consistent delivery of service to the buyer by a service provider.

The goals of this Agreement are to:

Provide clear reference to service ownership, accountability, roles and/or responsibilities.

Present a clear, concise and measurable description of service provision to the customer.

Establish Terms and Conditions for all the involved stakeholders.

To ensure that both the parties understand the consequences in case of termination of services due to any of the stated reasons

Thus, the agreement will act as a reference document that both the parties have understood the aforementioned terms and conditions and have agreed to comply by the same.

Service Scope

Cloud service can be used by the Government Organizations to hire the virtualized servers and other services such storage , network services and database licenses etc as depicted in child category offered by the Cloud Service Providers.

Cloud Has Established Its Monetary & Non-Monetary Benefits. Government Organizations Cannot Afford To Miss On-Boarding The Cloud Bandwagon If They Want To Deliver Their Services To Businesses And Consumers Resourcefully. However, Cloud Service Providers (CSPs), Operating In India, Have Been Offering Differing And Proprietary Cloud Services, And It Is Very Difficult For Government Organizations To Compare And Select Cloud Services That Can Meet Their Business And IT Requirements.

The Cloud Services Offered By The Global And Domestic CSPs Vary Significantly Even If The Services Are Intended To Cater To The Same Requirements Of The Government Organizations. The Input Parameters Required To Procure The Cloud Services And The Measurement / Monitoring Criteria Used To Bill The Service Consumers Also Vary Greatly.

In Order To Assist The Government Organizations In Selecting Appropriate Cloud Services From The Plethora Of Offerings Of CSPs, The Common IT Requirements Of Government Organizations Were Identified And An Attempt Has Been Made To Prepare A List Of Cloud Services, Which Are, To A Reasonable Extent, St[illegible] All CSPs. Though It Is Not Possible To Make An Apple To Apple Comparison Between C[illegible] l By Various CSPs, The Intent Of Providing This Bouquet Of Cloud Services Is To Make G[illegible]ations Aware Of The Common Cloud Services Which Are Being Offered By The Empanelled CSPs And Which Can Be Compared, To A Reasonable Extent, Across All CSPs, Before Taking The Decision To Procure A Cloud Service From A Particular CSP.

2.1. Special Terms and Conditions

Buyer Obligation:

Buyer will be governed by the relevant portion given in document published by Meity. For ready reference link of the document is reproduced as under

Guidelines on Master Service Agreement for procuring Cloud Services
Guidelines for User Departments on Service Level Agreement (SLA) for procuring Cloud services
Guidelines for Procurement of Cloud Services

Service Provider Obligation:

Cloud service provider must comply to the requirements in the offerings of Infrastructure as a Service and Platform as a Service as mentioned by Meity:

Guidelines on Master Service Agreement for procuring Cloud Services
Guidelines for User Departments on Service Level Agreement (SLA) for procuring Cloud services
Guidelines for Procurement of Cloud Services

Should adhere to the relevant standards published (or to be published) by MeitY or any standards body setup / recognised by Government of India and notified to the Service Provider by MeitY as a mandatory standard.

Service Provider shall also adhere to the relevant audit requirements as desired by users.

S nclude following offering/inclusion without any extra cost

[1] CSPs shall not charge any extra amount from the Government Departments other than the prices discovered for the Services consumed by the Government Departments.

[2] Discovered prices shall include all prices associated with consuming a service fully.

Guideline for onboarding Managed Service Provider is available in resource section of GeM Portal .

2.1.2. Payment Terms

The payment will happen monthly, quarterly, or annually as selected in the Service Order.

The monitoring software would help monitor the actual hours of usage in the selected time period and the billing would be adjusted as per actual usage for that billing cycle.

The deviation of usage hours mentioned during purchasing the service and the actuals should be within 25%.

Eligibility Criterion for Service Provider is as mentioned by MeitY

2.1.3. SLA and Penalty

For the Departments to ensure that the Cloud Service Providers adhere to the Service Level Agreements, this section describes the Penalties which may be imposed on CSPs. In case these service levels cannot be achieved at service levels defined in the agreement, the departments should invoke the performance related penalties. Payments to the SP to be linked to the compliance with the SLA metrics laid down in the agreement.

S.No#	Service Level Objective	Definition	Target	Penalty
Availability				

1	Availability of each cloud service (Applicable for all Cloud Service as defined in Cloud Services Bouquet)	Availability means, the aggregate number of hours in a calendar month during which cloud service is actually available for use through command line interface, user/admin portal and APIs(which ever applicable) Uptime Calculation for the calendar month: {[(Uptime Hours in the calendar month + Scheduled Downtime in the calendar month) / Total No. of Hours in the calendar month] x 100}	Availability for each of the cloud service>=99.5%	Penalty as indicated below (per occurrence): a) <99.5% to >= 99.00% - 10% of Quarterly Payment of the Project b) <99.00% to >= 98.50% - 15% of Quarterly Payment of the Project c) <98.50% to >= 98.00% - 20% of Quarterly Payment of the Project d) <98% - 30% of the Quarterly Payment of the Project In case the services is not available for a continuous period of 8 Business Hours on any day, penalty shall be 100% of the Quarterly Payment of the Project.

2	Availability of Critical Services(As defined in Annexure B) *This SLA shall not be applicable when the associated cloud service as mentioned in SLA#1 above is not available /up.	Availability means, the aggregate number of hours in any specified time period during which the critical service is actually available for use through command line interface, user/admin portal and APIs(which ever applicable) Uptime Calculation for the calendar month: {[(Uptime Hours in the calendar month + Scheduled Downtime in the calendar month) / Total No. of Hours in the calendar month] x 100}	Availability for each of the critical service>=99.5%	Penalty as indicated below (per occurrence): a) <99.5% to >= 99.00% - 5% of Quarterly Payment of the Project b) <99.00% to >= 98.50% - 10% of Quarterly Payment of the Project c) <98.50% to >= 98.00% - 15% of Quarterly Payment of the Project d) <98% - 20% of the Quarterly Payment of the Project In case the services is not available for a continuous period of 8 Business Hours on any day, penalty shall be 100% of the Quarterly Payment of the Project.

3	Availability of regular reports (SLA , Cloud Services Consumption, Monitoring, Billing and Invoicing, Security, & Project Progress)	Regular reports should be submitted to the Government dept. within 5 working days from the end of the month.	Regular reports should be submitted to the Government dept. within 5 working days from the end of the month.	Penalty as indicated below (per occurrence): a) <11 working days to >= 6 working days - 2% of Quarterly Payment for the Project b) <16 working days to >= 11 working days - 4% of Quarterly Payment for the Project c) For the delay beyond 15 days , penalty of 5% of the Quarterly Payment for the Project

4	Availability of the Cloud Management Portal of CSPs	Availability means the aggregate number of hours in a calendar month during which cloud management portal of CSP is actually available for use Uptime Calculation for the calendar month: {[(Uptime Hours in the calendar month + Scheduled Downtime in the calendar month) / Total No. of Hours in the calendar month] x 100}	Availability of the Cloud Management Portal of CSP >=99.5%	Penalty as indicated below (per occurrence): a) <99.5% to >= 99.00% - 10% of Quarterly Payment of the Project b) <99.00% to >= 98.50% - 15% of Quarterly Payment of the Project c) <98.50% to >= 98.00% - 20% of Quarterly Payment of the Project d) <98% - 30% of the Quarterly Payment of the Project In case the Cloud Management Portal of the CSP is not available for a continuous period of 8 Business Hours on any day, penalty shall be 50% of the Quarterly Payment of the Project.
Performance				

5	Provisioning of new Virtual Machine	Time to provision new Virtual Machine (up to 64 core) Measurement shall be done by analyzing the log files	95% within 5 minutes	Penalty as indicated below (per occurrence): a) <95% to >= 90.00% - 5% of Quarterly Payment of the Service b) <90% to >= 85.0% - 10% of Quarterly Payment of the Service c) <85% to >= 80.0% - 15% of Quarterly Payment of the Service d) <80% - 20% of the Quarterly Payment of that Service
6	Spinning up the Object Storage	Time to spin up Object Storage Measurement shall be done by analyzing the log files	98% within 15 minutes	Penalty as indicated below (per occurrence): a) <98% to >= 95.00% - 5% of Quarterly Payment of the Service b) <95% to >= 90.0% - 10% of Quarterly Payment of the Service c) <90% to >= 85.0% - 15% of Quarterly Payment of the Service d) <85% - 20% of the Quarterly Payment of that Service

Ask GeMmy

7	Spinning up the Block Storage	Time to spin up to 100 GB Block Storage and attach it to the running VM Measurement shall be done by analyzing the log files	98% within 15 minutes	Penalty as indicated below (per occurrence): a) <98% to >= 95.00% - 5% of Quarterly Payment of the Service b) <95% to >= 90.0% - 10% of Quarterly Payment of the Service c) <90% to >= 85.0% - 15% of Quarterly Payment of the Service d) <85% - 20% of the Quarterly Payment of that Service
8	Usage metric for all Cloud Services	The usage details for all the Cloud Service should be available within 15 mins of actual usage Measurement shall be done by analyzing the log files and Cloud Service (API) reports.	No more than 15 minutes lag between usage and Cloud Service (API) reporting, for 99% of Cloud Services consumed by the Government Dept.	Penalty as indicated below (per occurrence): a) <99% to >= 95.00% - 1% of Quarterly Payment of the Project b) <95% to >= 90.0% - 2% of Quarterly Payment of the Project c) <90% to >= 85.0% - 3% of Quarterly Payment of the Project d) <85% - 5% of the Quarterly Payment of that Project

9	Usage cost for all Cloud Service	The cost details associated with the actual usage of all the Cloud Service should be available within 24Hrs of actual usage Measurement shall be done by analyzing the log files and Cloud Service (API) reports and Invoices	No more than 24 Hrs. of lag between availability of cost details and actual usage, for 99% of Cloud Services consumed by the Government Dept.	Penalty as indicated below (per occurrence): a) <99% to >= 95.00% - 1% of Quarterly Payment of the Project b) <95% to >= 90.0% - 2% of Quarterly Payment of the Project c) <90% to >= 85.0% - 3% of Quarterly Payment of the Project d) <85% - 5% of the Quarterly Payment of that Project
Security				
11	Percentage of timely vulnerability reports	Percentage of timely vulnerability reports shared by CSP/MSP with Government Dept. within 5 working days of vulnerability identification. Measurement period is calendar month.	Percentage of timely vulnerability reports shared with Government Dept. within 5 working days of vulnerability identification>= 99.95%	Penalty as indicated below (per occurrence): a) <99.95% to >= 99.00% - 10% of Quarterly Payment for the Project b) <99.00% to >= 98.00% - 20% of Quarterly Payment for the Project b) <98% - 30% of Quarterly Payment for the Project

Ask GeMmy

12	Percentage of timely vulnerability corrections	Percentage of timely vulnerability corrections performed by CSP/MSP. a) High Severity - Perform vulnerability correction within 30 days of vulnerability identification. b) Medium Severity - Perform vulnerability correction within 60 days of vulnerability identification. c) Low Severity - Perform vulnerability correction within 90 days of vulnerability identification. Measurement period is calendar month.	Maintain 99.95% service level	Penalty as indicated below (per occurrence): a) <99.95% to >= 99.00% - 10% of Quarterly Payment for the Project b) <99.00% to >= 98.00% - 20% of Quarterly Payment for the Project b) <98% - 30% of Quarterly Payment for the Project

13	Security breach including Data Theft/Loss/Corruption	Any incident wherein system including all cloud based services and components are compromised or any case wherein data theft occurs (includes incidents pertaining to CSPs only)	No breach	For each breach/data theft, penalty will be levied as per following criteria. 1. Severity 1 (as define in Annexure A) - Penalty of Rs 15 Lakh per incident. 2. Severity 2 (as define in Annexure A) - Penalty of Rs 10 Lakh per incident. 3. Severity 3 (as define in Annexure A) - Penalty of Rs 5 Lakh 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.

Ask GeMmy

15	Security Incident (Malware Attack/ Denial of Service Attack/ Data Theft/ Loss of data/ Intrusion or Defacement) Applicable on the CSP's underlying infrastructure	Security incidents could consist of any of the following: Malware Attack: This shall include Malicious code infection of any of the resources, including physical and virtual infrastructure and applications. Denial of Service Attack: This shall include non-availability of any of the Cloud Service due to attacks that consume related resources. The Service Provider shall be responsible for monitoring, detecting and resolving all Denial of Service (DoS) attacks. Intrusion: Successful unauthorized access to system, resulting in loss of confidentiality/ Integrity/availability of data. The Service Provider shall be responsible for monitoring, detecting and resolving all security related intrusions on the network using an Intrusion Prevention device.	a) Any Denial of service attack shall not lead to complete service non-availability. b) Zero Malware attack / Denial of Service attack / Intrusion / Data Theft	For each occurrence of any of the attacks (Malware attack / Denial of Service attack / Intrusion / Data Theft), 10% of the Quarterly Payment of the Project

Support Channels - Incident and Helpdesk

16	Response Time under Basic Support (As defined under cloud service bouquet)	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 60 minutes	a) <95% to >= 90.00% - 5% of Quarterly Payment of Basic Support service b) <90% to >= 85.00% - 7% of Quarterly Payment of Basic Support service c) <85% to >= 80.00% - 9% of Quarterly Payment of Basic Support service d) Subsequently, for every 5% drop in SLA criteria - 2% of Quarterly Payment of Basic Support service
17	Percentage of timely incident report under Basic Support service(As defined under cloud service bouquet)	The defined incidents to the cloud service which are reported to the Government Dept. in a timely fashion. This is represented as a percentage by the number of defined incidents reported within 1 hr. after discovery in a month, over the total number of defined incidents to the cloud service which are reported within the month	95% of the incidents should be reported to Government Dept. within 1 Hr. of occurrence.	a) <95% to >= 90.00% - 5% of Quarterly Payment of Basic Support service b) <90% to >= 85.00% - 10% of Quarterly Payment of Basic Support service c) <85% to >= 80.00% - 15% of Quarterly Payment of Basic Support service d) Subsequently, for every 5% drop in SLA criteria - 5% of Quarterly Payment of Basic Support service

18	Response Time under Enterprise Support (As defined under cloud service bouquet)	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 15 minutes	a) <95% to >= 90.00% - 5% of Quarterly Payment of Enterprise Support service b) <90% to >= 85.00% - 7% of Quarterly Payment of Enterprise Support service c) <85% to >= 80.00% - 9% of Quarterly Payment of Enterprise Support service d) Subsequently, for every 5% drop in SLA criteria - 2% of Quarterly Payment of Enterprise Support service

19	Percentage of timely incident report under Enterprise Support service(As defined under cloud service bouquet)	The defined incidents to the cloud service which are reported to the Government Dept. in a timely fashion. This is represented as a percentage by the number of defined incidents reported within 1 hr. after discovery in a month, over the total number of defined incidents to the cloud service which are reported within the month	95% of the incidents should be reported to Government Dept. within 15 min of occurrence.	a) <95% to >= 90.00% - 5% of Quarterly Payment of Enterprise Support service b) <90% to >= 85.00% - 10% of Quarterly Payment of Enterprise Support service c) <85% to >= 80.00% - 15% of Quarterly Payment of Enterprise Support service d) Subsequently, for every 5% drop in SLA criteria - 5% of Quarterly Payment of Enterprise Support service
20	Time to Resolve - Severity 1	Time taken to resolve the reported ticket/incident from the time of logging.	For Severity 1, 95% of the incidents should be resolved within 30 minutes of problem reporting	a) <95% to >= 90.00% - 5% of Quarterly Payment of the Project b) <90% to >= 85.00% - 10% of Quarterly Payment of the Project c) <85% to >= 80.00% - 15% of Quarterly Payment of the Project d) Subsequently, for every 5% drop in SLA criteria - 5% of Quarterly Payment of the Project

21	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 AND 95% of Severity 3 within 16 hours of problem reporting	a) <95% to >= 90.00% - 5% of Quarterly Payment of the Project b) <90% to >= 85.00% - 10% of Quarterly Payment of the Project c) <85% to >= 80.00% - 15% of Quarterly Payment of the Project d) Subsequently, for every 5% drop in SLA criteria - 5% of Quarterly Payment of the Project
Disaster Recovery and Data Backup Management				
22	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.	RTO <= 4 hours Government Department may specify more stringent RTO based on its application requirements	10% of Quarterly Payment of the Project per every additional 2 (two) hours of downtime
23	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.	RPO <= 2 hours Government Department may specify more stringent RPO based on its application requirements	10% of Quarterly Payment of the Project per every additional 2 (two) hours of data loss

24	DR Drills	At least two DR drills in a year (once every six months) or as per the agreement	At least two DR drills in a year (once every six months) or as per the agreement	a) No of DR Drills =1 - 1% of the Yearly Payment of the Project b) No of DR Drills = 0 - 2% of the Yearly Payment of the Project These will be measured every six months and the liquidated damage will be levied at the end of year
25	Data Migration	Migration of data from the source to destination system	Error rate < .25%	a) Error Rate > 0.25% & <=0.30% - 1% of the Quarterly Payment of the Project b) Error Rate > 0.30% & <=0.35% - 2% of the Quarterly Payment of the Project c) Error Rate > 0.35% & <=0.40% - 3% of the Quarterly Payment of the Project For each additional drop of 0.05% in Error rate after 0.40%, 1% of Total Quarterly Payment of the Project will be levied as additional liquidity damage

Audit & Monitoring

26	Patch Application	Patch Application and updates to underlying infrastructure and cloud service Measurement shall be done by analyzing security audit reports	95% within 8 Hrs. of the notification	Penalty as indicated below (per occurrence): a) <95% to >= 90.00% - 5% of Quarterly Payment of the Project b) <90% to >= 85.0% - 10% of Quarterly Payment of the Project c) <85% to >= 80.0% - 15% of Quarterly Payment of the Project d) <80% - 20% of the Quarterly Payment of that Project
27	Budget Alerts & Notification	Alerts and Notifications for budgeting and usage based threshold Measurement shall be done by analyzing the log files	99% within 10 mins of crossing the Threshold	Penalty as indicated below (per occurrence): a) <99% to >= 95.00% - 0.25% of Quarterly Payment of the Project b) <95% to >= 90.0% - 0.5% of Quarterly Payment of the Project c) <90% to >= 85.0% - 0.75% of Quarterly Payment of the Project d) <85% - 1% of the Quarterly Payment of that Project

28	Audit of the Sustenance of Certifications	No certification (including security related certifications mandated under MeitY empanelment such as ISO27001, ISO27017, ISO27018, ISO20001 etc.) should lapse within the Project duration. Service Provider should ensure the sustenance / renewal of the certificates	All certificates should be valid during the Project duration	Delay in sustenance of certifications a) > 1 day & <= 5 days - 1% of the Quarterly Payment of the Project b) > 5 day & <= 15 days - 2% of the Quarterly Payment of the Project c) > 15 day & <= 30 days - 5% of the Quarterly Payment of the Project d) > 30 days, 10% of the Quarterly Payment of the Project
29	Non-closure of audit observations	No observation to be repeated in the next audit	All audit observations to be closed within defined timelines	Penalty for percentage of audit observations repeated in the next audit a) > 0 % & <= 10% - 5% of the Quarterly Payment of the Project b) > 10 % & <= 20% - 10% of the Quarterly Payment of the Project c) > 20 % & <= 30% - 20% of the Quarterly Payment of the Project d) >30% - 30% of the Quarterly Payment of the Project

Severity Levels

Below severity definition provide indicative scenarios for defining incidents severity. However Government Department/Agency will define / change severity at the time of the incident or any time before the closure of the ticket based on the business and compliance impacts.

Severity Level	Description	Examples
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.	

Ask GeMmy

Definitions

1. **Critical Services:** Critical service may be defined as Register Support Request or Incident; Provisioning / De-Provisioning; User Activation / De-Activation; User Profile Management; Security Components, etc.

1. **Business Hours**: Business hours may be referred as prime business period, which shall be from 08:00 A.M IST till 10:00 PM IST on all days.

Ask GeMmy