Inviting Application

for

Empanelment of Cloud Service Offerings of Cloud Service Providers

Ministry of Electronics and Information Technology

Electronics Niketan, 6, CGO Complex

New Delhi-110 003

May ' 2020

This Page is Intentionally Left Blank

Table of Contents

1. Background and Glossary of Terms 5

1.1. Background 5

1.2. Glossary of Terms 6

2. Purpose of the Application 8

3. Issuing Authority 9

4. Calendar of Events ..... Error! Bookmark not defined.

5. Cloud Services Empanelment Process for CSPs 10

6. Technical Requirements 13

6.1. Cloud Deployment Models 13

6.2. Cloud Service Models 21

6.3. Compliance Requirements 44

7. Governance Structure and Roles of the Different Agencies 45

8. Instructions to Applicants 47

9. Process of Evaluation 55

10. General Conditions 58

11. Annexure – 1 - Application Response Cover Letter 63

12. Annexure – 2 - Acceptance to offer Basic Cloud Services as defined in Cloud Services Bouquet of MeitY 67

13. Annexure – 3 - Basic Cloud Services Empanelment Form 68

14. Annexure – 4 - Advanced Cloud Services Empanelment Form 69

15. Annexure – 5 - Pre-Qualification Criteria 70

16. Annexure – 6 - Form for Submission of Pre-qualification Information 72

17. Annexure – 7 - Form for Submission of Technical Compliance 76

18. Annexure – 8 - Undertaking on Absence of Conflict of Interest..... 77

19. Annexure – 9 - Undertaking on Legal Compliance 78

20. Annexure – 10 - Format for Requirement Compliance Matrix 79

21. Annexure – 11 - Undertaking on Data Center Service Arrangements.....80

22. Annexure – 12 - Request for Clarification Format..... 82

23. Annexure – 13 - Compliance and Certification Requirements 83

24. Annexure – 14 - Format for Earnest Money Deposit (EMD) 84

25. Annexure – 15 - Cloud Services Bouquet..... 86

25.1 Basic Cloud Services 87

25.1.1 Compute Services 87
25.1.2 Storage Services 91
25.1.3 Database Services 94
25.1.4 Network Services 95
25.1.5 Security Services 99
25.1.6 Support Services 101

25.2 Advanced Cloud Services 102

25.2.1 Compute Services 102
25.2.2 Database Services 103
25.2.3 Network Services 107
25.2.4 Security Services 109
25.2.5 Monitoring Services 112
25.2.6 Office Productivity Suit 115
25.2.7 Analytics Services 116

25.3 Managed Services 118

25.3.1 Disaster Recovery as a Service (DRaaS) 118
25.3.2 Backup as a Service 122

1. Background and Glossary of Terms

1.1. Background

Ministry of Electronics & Information Technology (MeitY) conducted two rounds of empanelment of Cloud Service Offerings by Cloud Service Providers (CSPs) in year 2016 and 2017. The Cloud Service Offerings of CSPs were empaneled for three different Cloud Deployment Models namely, Public Cloud, Virtual Private Cloud, and Government Community Cloud for a period of two years with an extension for one more year. The empanelment period of all the existing CSPs has been extended at least till September 2022, post successful STQC audit.

To empanel the service offerings of new CSPs (whose services are not yet empaneled with MeitY), MeitY invites applications from such prospective Cloud Service Providers. This document provides empanelment requirements and guidelines for Cloud services across the three Cloud Deployment Models and three Cloud Service Models namely, Infrastructure as a Service (IaaS), Platform as a Service (PaaS) and Software as a Service (SaaS).

1.2. Glossary of Terms

Acronym	Expansion
MeitY	Ministry of Electronics and Information Technology
GOI	Government of India
CSP	Cloud Service Providers
PBG	Performance Bank Guarantee
GI Cloud	Government of India Cloud
IaaS	Infrastructure as a Service
PaaS	Platform as a Service
SaaS	Software as a Service
RPO	Recovery Point Objective
RTO	Recovery Time Objective
SLA	Service Level Agreement
PC	Public Cloud
VPC	Virtual Private Cloud
GCC	Government Community Cloud
ISO	International Organization for Standardization
DR	Disaster Recovery
DC	Data Centre
STQC	Standardization Testing and Quality Certification
GeM	Government e-Marketplace
PSU	Public Sector Undertaking
UT	Union Territory
VLAN	Virtual Local Area Network
VMs	Virtual Machines
DDOS	Distributed Denial of Service
CERT-IN	Indian Computer Emergency Response Team
OS	Operating System
SSL	Secure Socket Layer
TLS	Transport Layer Security
SSH	Secure Shell
API	Application Programming Interface
CPU	Central Processing Unit
RAM	Random Access Memory

Acronym	Expansion
ITIL	Information Technology Infrastructure Library
N/W	Network
CRUD	Create, Read, Update, Delete
LAN	Local Area Network
WAN	Wide Area network
DHCP	Dynamic Host Configuration Protocol
VPN	Virtual Private Network
MPLS	Multiprotocol Label Switching
ISP	Internet Service Provider
AD	Active Directory
NOC	Network Operations Centre
SOC	Securities Operation Centre
DRDC	Disaster Recovery Data Centre

2. Purpose of the Application

The primary purpose of this application is to empanel the cloud service offering of the Cloud Service Providers (whose services are not yet empaneled by MeitY). From now onwards, the 'CSP' / 'Cloud Service Provider' as mentioned in this document shall refer to only new CSPs (Cloud Service Providers), whose services have not been empaneled with MeitY. In the new empanelment process, detailed audit of each CSP shall be conducted before its services are empaneled with MeitY. This empanelment shall be valid for a duration as mentioned in the Section 10 – 'Process of Evaluation'. Thereafter, each CSP shall also undergo a surveillance audit every periodically every year for the following two requirements.

(i) Minimum security requirements specified by MeitY

(ii) Any additional requirements specified by MeitY / requirements arising out of any additional service proposed to be offered by the CSP

MeitY invites applications from the CSPs (hereinafter referred to as "Applicants") for empaneling their Cloud Service Offerings for a combination of the Cloud Deployment Models (Public Cloud, Virtual Private Cloud, Government Community Cloud) and Cloud Service Models (Infrastructure as a Service, Platform as a Service, and Software as a Service). In addition, existing CSPs whose services are empaneled by MeitY may enroll additional Data Center sites and services under this empanelment application. This shall also be considered as a fresh application and CSPs must follow the process stated in the application document.

The CSPs shall be required to offer the Cloud services according to the Cloud Services Bouquet prepared by MeitY. In the bouquet, the Cloud services have been categorized into "Basic Cloud Services" and "Advanced Cloud Services" (referAnnexure 15 – Cloud Services Bouquet). The Cloud services listed under the "Basic Cloud Services" are mandatory for all CSPs to offer to the government organizations under at least one of the empaneled Cloud Deployment Models. However, the Cloud services listed under the "Advanced Cloud Services" category are optional for the CSPs to offer.

The 'Invitation for Application' is not an offer by MeitY but an invitation to receive proposals from eligible and interested Applicants in respect of the requirements mentioned in this document. The Application/Proposal does not commit MeitY to enter into a binding agreement in respect of the project with the potential Applicants.

3. Issuing Authority

This Application document for Cloud services empanelment is issued by the Ministry of Electronics and Information Technology (MeitY) and is intended to empanel Cloud Service Offerings by the Cloud Service Providers. MeitY's decision with regard to empanelment of the Cloud Service Offerings through this proposal shall be final.

S. No.	Item	Description
1	Project Title	Inviting Application for Empanelment of Cloud Service Offerings of Cloud Service Providers
	Project Initiator and Issuer Details	
2	Department / Ministry	Ministry of Electronics and Information Technology (MeitY)
3	Contact Person	KshitijKushagra Scientist E/Addl. Director Ministry of Electronics and Information Technology Electronics Niketan, 6, CGO Complex New Delhi-110 003 Tel: +91-11-24301373
4	Contact Person (Alternate)	Uma Chauhan Scientist F/ Director Ministry of Electronics and Information Technology Electronics Niketan, 6, CGO Complex New Delhi-110 003 Tel: +91-11-24364711
5	Email address for all application/proposal correspondence	kshitij.kushagra@meity.gov.in
6	Address for the purpose of application/proposal submission	KshitijKushagra Scientist E/ Addl. Director CR Section, Ground Floor Ministry of Electronics and Information Technology, Electronics Niketan, 6, CGO Complex New Delhi-110 003 Tel: +91-11-24301373
7	MeitY website	http://meity.gov.in/

4. Calendar of Events

The following table enlists important milestones and timelines for completion of activities:

S. No.	Milestone	Date and Time	Remark in case Applicants doesn't meet the timeline
1	Publishing of the Application	21.05.2020	Application document publish
2	Application Submission last date	20.07.2020	No application will be considered beyond the Application submission window.

Note- The empanelment window is opened for two months, the applicant can submit their application within the time frame from 21.05.2020 to 20.07.2020.

5. Cloud Services Empanelment Process for CSPs

The complete process of Cloud Services Empanelment is as follows:

Step 1 - Cloud Service Details by CSP: CSPs shall submit the details of proposed individual services as per Cloud Services Bouquet at the time of submission of application, along with the details of relevant Cloud Deployment Models and Cloud Service Models. The "Basic Cloud Services" are mandatory for all CSPs to offer to the government organizations under at least one of the empaneled Cloud Deployment Models. However, the "Advanced Cloud Services" are optional for the CSPs to offer. The details of the Cloud Service Offerings for empanelment shall be provided by the CSPs in the prescribed format as per Annexure – 3 and Annexure – 4.

Step 2 - Application assessment by MeitY: MeitY shall conduct the compliance check and initial assessment to ascertain that the CSP has submitted all the required documents as mentioned in this invitation document. Post successful assessment, the application shall be submitted to STQC.

Step 3 - Audit by STQC: It shall be the responsibility of individual CSPs to get their Data Centers and Cloud Service Offerings successfully audited by STQC.

(i) On successful application assessment by MeitY, STQC will seek the required documents from the CSP for auditing its Data Center(s) and Cloud Service Offerings. Each CSP shall be required to furnish the sought documents and the Audit Fee in a week's time.

(ii) STQC shall audit the Data Center(s) and Cloud Service Offerings of each CSP within a shortest possible time.

(iii) STQC shall inform MeitY of the status of audit of Data Center(s) and Cloud Service Offerings of each CSP.

Step 4 – Declaration of Empaneled Cloud Services by MeitY: MeitY shall publish the list of Cloud services and Data Center facilities of each CSP, successfully audited by STQC on the GI Cloud MeghRaj webpage available on the MeitY website.

(i) In case of a successful audit by STQC, MeitY shall issue a Letter of Award of Empanelment to the CSP clearly mentioning the Cloud Service Offerings and Cloud Deployment Models successfully empaneled with MeitY. The letter shall also specify the Data Center(s) facility from which the empaneled Cloud services can be offered to the government organizations.

(ii) The empaneled Cloud Service Offerings and Cloud Deployment Models, along with the Data Center (s) facility, of the CSP shall be listed on the GI Cloud Portal / MeghRaj webpage available on the MeitY website

(iii) In case non-compliances are found during the audit conducted by the STQC, the CSP shall be notified/informed about this and advised to address these non-compliances. The CSP shall address these non-compliances and reapply for the STQC Audit within one week of the receipt of notification of the non-compliances. In case the CSP applies for re-audit of similar non-compliances more than 2 times, the CSP application for the current empanelment will stand cancelled and they will have to re-apply in the next empanelment cycle.

Step 5 – Providing Empaneled Cloud Services through GeM: The CSPs shall offer the empaneled Cloud services to government organizations through GeM platform.

(i) MeitY shall inform GeM team about the empaneled Cloud Service Offerings of CSPs.

(ii) CSPs whose Cloud services are successfully empaneled with MeitY shall onboard these services on the GeM platform as per the directions provided by the GeM team.

(iii) Government organizations may procure these empaneled Cloud services from the GeM Marketplace or through the Bid / Reverse Auction facility available on the GeM platform.

6. Technical Requirements

The minimum indicative technical requirements as described in the sections below shall be complied by Cloud Service Providers (CSPs) to get their Cloud Services empaneled in accordance to the technical and compliance requirements as specified in this document.

6.1. Cloud Deployment Models

The CSP shall be responsible to meet the below requirements in accordance with the Public Cloud, Virtual Private Cloud and Government Community Cloud

6.1.1. Requirements Specific to Cloud Deployment Models

The below requirements as specified in the table are specific to Cloud Deployment Model and CSPs shall be required to meet the requirements to offer Cloud Services from the respective Cloud Deployment Model.

- Clause 6.1.1.A refers to the 'Requirement(s)' for Public Cloud Deployment Model detailed below.
- Clause 6.1.1.B refers to the 'Requirement(s)' for Virtual Private Cloud Deployment Model detailed below.
- Clause 6.1.1.C refers to the 'Requirement(s)' for Government Community Cloud Deployment Model detailed below.

Requirement(s)	Public Cloud (A)	Virtual Private Cloud (B)	Government Community Cloud (C)
1. Government Community Cloud shall only offer Cloud services to Govt. Departments / Ministries / Agencies / Autonomous Institutions / Statutory Bodies / Offices under Government of India or States or UTs or Local Governments or PSUs or Nationalized Banks within India (herein after referred to as Government Department).	N	N	Y
2. CSP shall ensure that GCC environment is operational with minimum 5 numbers of 42U racks covering Network, Storage, Compute and Security components, for immediate use at the time of submission of application for empanelment.	N	N	Y

Requirement(s)	Public Cloud (A)	Virtual Private Cloud (B)	Government Community Cloud (C)
3. The services shall be provided on a logical dedicated Cloud (herein after referred to as Virtual Private Cloud) at the Data Center.	N	Y	N
4. The infrastructure elements including physical server, physical storage (including backup storage), network infrastructure, and IT security for the Government Community Cloud shall be dedicated to the Government Department solutions and shall be physically separate from the public and other Cloud offerings of the Cloud Service Providers. There should be physical and logical separation (of space, servers, storage, network infrastructure and security) to protect data, applications and servers. However, the dedicated infrastructure elements can be shared by the Government Departments.	N	N	Y
5. Virtual Private Cloud environment shall be usedto offer onlyCloud services for Departments / Ministries / Agencies / Autonomous Institutions / Statutory Bodies / Offices under Government of India or States or UTs or Local Governments or PSUs or Nationalized Banks within India (herein after referred to as Government Department)	N	Y	N
6. The space allocated for the dedicated infrastructure shall be clearly demarcated and identified as hosting Government Department's Projects. The demarcated and identified area shall not host any components other than those of Government Departments Projects.	N	N	Y
7. The infrastructure elements including server, storage (including backup storage) and network of the Virtual Private Cloud should			

Requirement(s)	Public Cloud (A)	Virtual Private Cloud (B)	Government Community Cloud (C)
provide strong tenant isolation, provide granular identity and access management capability and encryption and be logically separate from the public and other Cloud offerings of the Cloud Service Provider. There should be logical separation (of servers, storage, network infrastructure and networks) to protect data, applications and servers and provide robust virtual isolation for the Virtual Private Cloud.	N	Y	N
8. The entire N/W Path for each of the hosted government applications shall be separate (logical separation & isolation) from the other clients (including other government departments) and should be dedicated for the respective Government Department.	N	Y	Y
9. The CSP shall implement a firewall policy that allows the Government Department to administer it remotely or shall administer a firewall policy in accordance with the Government Department's direction, allowing the Department to have read-only access to inspect the firewall configuration.	N	Y	Y
10. The Cloud service offering shall support Network and security with virtual firewall and virtual load balancer integration for auto-scale functions.	Y	Y	N
11. The Cloud service offering shall support Network and security with dedicated firewall and load balancer integration for auto-scale functions. However, the dedicated infrastructure elements can be shared by the Government Departments.	N	N	Y
12. Must have Separate VLAN provision with dedicated firewall between the VLANs and for	N	Y	N

Requirement(s)	Public Cloud (A)	Virtual Private Cloud (B)	Government Community Cloud (C)
each and every client on the Virtual Private Cloud.			
13. Must have Separate VLAN provision with dedicated firewall between the VLANs and for each and every client on the Government Community Cloud.	N	N	Y
14. The management consoles shall only show the data relevant for the Government Department.	Y	Y	Y
15. The management consoles for the dedicated Government Community Cloud shall only show data for the dedicated Government Community Cloud and in the same manner, the monitoring data of dedicated Government Community Cloud shall not be available on any other management console.	N	N	Y
16. With respect to monitoring tools, if any agent has to be deployed on the VMs or otherwise, the monitoring tools may be shared, provided there is logical segregation and controls built-in to ensure that the tools and deployed agents comply with the security policies. Only the events, performance threshold alerts and inventory data for the OS, DB, infrastructure and Application is captured & sent by the deployed agents. The monitoring tools and deployed agents (in case of agent-based tools) shall not capture or send Government Department's application and/or user and/or transaction data	Y	Y	Y
17. All the physical, environmental and security features, compliances and controls of the Data Center facilities (as required under this application document) shall be enabled for the Cloud Service Offerings	Y	Y	Y

Requirement(s)	Public Cloud (A)	Virtual Private Cloud (B)	Government Community Cloud (C)
18. Shall leverage and share all network related security toolset which are in network flow. However, host-based security like IDS, PIM, FIM should be specific to Virtual Private Cloud.	N	Y	N
19. Security toolset except DDOS, shall be a dedicated installation of the tools / products for the Government Community Cloud. DDOS need not be a dedicated installation for the Government Community Cloud and may be deployed as a shared service.	N	N	Y
20. Cloud provisioning toolset can be shared tools.	Y	Y	N
21. In case, the CSP provides Database System Software as a Service for the Government Department, the database shall be a dedicated installation for the User Department Government Community Cloud.	N	N	Y
22. In case, the CSP provides Database System Software as a Service for the Government Department, the database shall be a dedicated installation for the User Department Virtual Private Cloud.	N	Y	N
23. For ensuring strategic control of the operations, the CSP shall provide self-service tools to the Government Departments that can be used to manage their Cloud infrastructure environments including Government Department specific configurations	Y	Y	Y
24. For ensuring strategic control of the operations, approval of MeitY /Government Departments shall be taken prior to making changes / modifications of the deployed			

Requirement(s)	Public Cloud (A)	Virtual Private Cloud (B)	Government Community Cloud (C)
solution, database, data, configurations, security solutions, hosted infrastructure, etc. of the Government Community Cloud where such changes affect solutions of multiple Government Departments using the Government Community Cloud. The above set of activities where prior approvals of the MeitY have to be taken is only indicative and by no means an exhaustive list. The set of activities for which such approval has to be obtained will be finalized by MeitY/Government Department and reviewed on as needed basis.	N	N	Y
25. Where required, MeitY or the Government Department as applicable, shall be provided the access rights on the Cloud services console that will enable empaneled MeitY user or Government Department user, as applicable, to approve any critical changes to the solution including the underlying infrastructure before they are carried out by the CSP	N	N	Y
26. For any changes (including auto-provisioning and others that may or may not need prior approval) to the underlying Cloud infrastructure, software, etc. under the scope of the CSP that has the potential to affect the SLAs (performance, availability,..), the Government Department shall get alerts / notifications from the CSP, both as advance alerts and post implementation alerts.	Y	Y	Y

6.1.2. General Requirements for all Cloud Deployment Model

The below mandatory requirements are applicable for all Cloud Deployment Models i.e. Public Cloud, Virtual Private Cloud and Government Community Cloud

1. There should be sufficient headroom (at an overall level in the compute, network, and storage capacity offered) available for near real time provisioning (as per the SLA requirement of the Government Department) during any unanticipated spikes in the user load. The provisioning / de-provisioning SLAs may differ for the different Cloud Deployment Models.

2. Ability to integrate fully with the Government of India approved Certificate Authorities to enable the Government Departments use the Digital Certificates / Digital Signatures.

3. The respective Government Department shall retain ownership of any user created/loaded data and applications hosted on CSP's infrastructure and maintains the right to request (or should be able to retrieve) full copies of these at any time.

4. The respective Government Department retains ownership of all virtual machines, templates, clones, and scripts/applications created for the department's application. The respective Government Department retains the right to request (or should be able to retrieve) full copies of these virtual machines at any time.

5. The respective Government Department retains ownership of Department loaded software installed on virtual machines and any application or product that is deployed on the Cloud by the Government Department.

6. The respective Government Department shall be provided access rights (including the underlying secure connection) to the user administration / portal of Cloud services to have visibility into the dashboard, SLAs, management reports, etc. provided by the Cloud Service Providers.

7. CSP shall not provision any unmanaged VMs for the applications.

8. CSPs shall provide interoperability support with regards to available APIs, data portability etc. for the Government Department to utilize in case of Change of Cloud Service Providers, migration back to in-house infrastructure, burst to a different Cloud Service Providers for a short duration or availing backup or DR services from a different service provider.

9. CSPs shall adhere to the ever-evolving guidelines as specified by CERT-In (http://www.cert-in.org.in/)

10. CSPs shall also adhere to the relevant audit requirements as defined in the application document or any new requirement as published by MeitY or STQC.

12. CSPs need to adhere to the guidelines and acts published by Government of India. No data should be shared to any third party without explicit approval by the User Department, unless legally required to do so by the courts of India. The empaneled Cloud services shall have to comply with the guidelines & standards as and when published by Govt. of India. CSPs shall be responsible for all costs associated with implementing, assessing, documenting, and maintaining the empanelment, any guidelines published by MeitY shall be followed by the CSPs. In case any misconduct is found, MeitY/ User Department reserves the right to take appropriate legal course of action including blacklisting of the CSP.

13. In case of any delay in publishing guidelines / standards by MeitY or identification of any critical gaps or deemed as required by MeitY during the period of empanelment, additional guidelines / standards may be published by MeitY from time to time that will be applicable for the empaneled Cloud Service Offerings of the Cloud Service Providers. The empaneled Cloud Service Offerings must comply with the additional guidelines / standards (applicable for the empaneled Cloud Service Offerings) as and when MeitY publishes such guidelines / standards, at no additional cost to retain the empanelment status. Cloud Service Providers shall be given sufficient time and notice period to comply with the additional guidelines / standards. Any downtime during such approved upgrades shall be considered as approved downtime for SLA calculations.

6.2. Cloud Service Models

The Cloud services offered by the CSPs can be offered from different Cloud Service Models. CSPs shall be required to offer their services as per the Cloud Service Bouquet prepared by MeitY. While applying for the empanelment of the Cloud services, CSPs shall be required to specify the Cloud Service Models as defined below, for each of the Cloud services that they wish to get empaneled with MeitY.

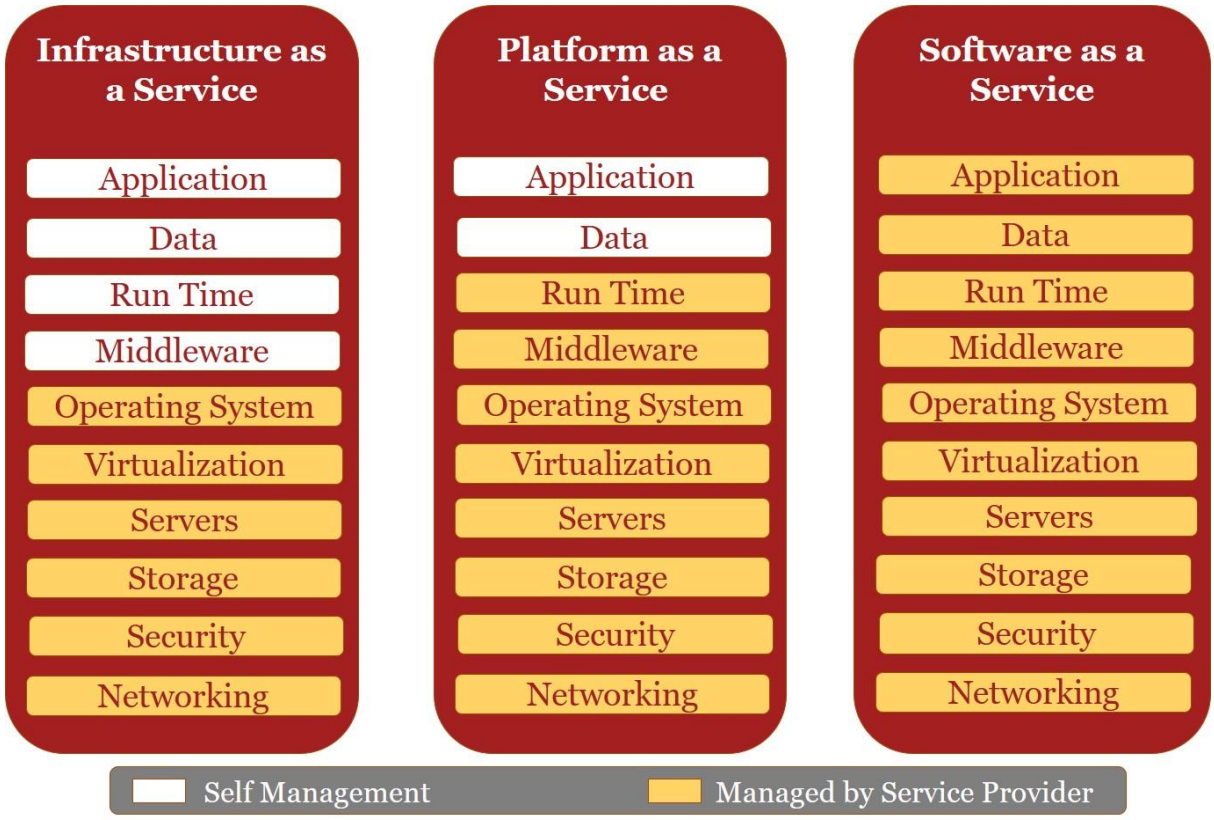

Figure 1: Cloud Service Models

1. **Infrastructure as a Service (IaaS):**The CSP shall provide the User Department with processing, storage, networks, and other fundamental computing resources where the consumer is able to deploy and run arbitrary software/application. The CSP shall be responsible for managing and controlling the underlying Cloud infrastructure including operating systems, storage, network, security, etc. and the deployed applications shall be managed and controlled by the User Department.

2. **Platform as a Service (PaaS):** The CSP shall provide the User Department the Cloud infrastructure and platform (such as middleware) to run the applications created using programming languages, libraries, services, and tools supported by the CSP. The user department shall not manage or control the underlying Cloud infrastructure including network, security, servers, operating systems, or storage, but has control over the deployed applications and possible configuration settings for the application-hosting environment.

3. **Software as a Service (SaaS):** The CSP shall offer its applications running on the Cloud infrastructure as services to User Departments. The applications shall be accessible from various client devices through either a thin client interface, such as a web browser or through a programming interface. The User Department shall not manage or control the underlying Cloud infrastructure, platform and application landscape including network, security, servers, operating systems, storage, or even individual application capabilities with the possible exception of limited user-specific application configuration settings.

6.2.1. Specific Requirements for 'Infrastructure as a Service' (IaaS)

The below mandatory requirements are applicable for services offered by CSP under 'Infrastructure as a Service', using Government Community Cloud or Virtual Private Cloud or Public Cloud. These are in addition to the General Requirements for all Cloud Deployment Models and all Cloud Services Model.

The CSPs shall be responsible for all activities, roles, and responsibilities for services being offered using Infrastructure as a Service as defined in Figure-1 of this document.

1. The CSPs shall make the services available online, on-demand and dynamically scalable up or down as per request for service from the end users (Government Department or Government Department's nominated agencies) with two-factor authentication via the SSL through a web browser.

2. The Service shall provide auto-scalable, redundant, dynamic computing capabilities or virtual machines.

3. Service shall allow Government Department empaneled users to procure and provision computing services or virtual machine instances online with two-factor authentication via the SSL through a web browser.

4. Service shall allow users to securely and remotely, load applications and data onto the computing or virtual machine instance from the SSL VPN clients only as against the public internet.

5. Perform an Image backup of Customer VM Image information or support the ability to take an existing running instance or a copy of an instance and export the instance into User Department(s) required format.

6. Configuration and Management of the Virtual Machine shall be enabled via a Web browser over the SSL VPN clients only as against the public internet.

7. In case of suspension of a running VM, the VM shall still be available for reactivation for a reasonable time without having to reinstall or reconfigure the VM for the Government Department solution. In case of suspension beyond a reasonable time, all the data within it shall be immediately deleted / destroyed and certify the VM and data destruction to the Government Department as per stipulations and shall ensure that the data is not forensically recovered.

8. CSP shall ensure that VMs receive OS patching, health checking and backup functions.

9. Monitor VM up/down status and resource utilization such as RAM, CPU, Disk, IOPS and network.

10. The respective Government Department shall retain ownership of all virtual machines, templates, clones, and scripts/applications created for the department's application. The respective Government Department retains the right to request (or should be able to retrieve) full copies of these virtual machines at any time.

11. The respective Government Department retains ownership of Department loaded software installed on virtual machines and any application or product that is deployed on the Cloud by the Government Department.

12. CSPs shall manage CSP provisioned infrastructure including VMs as per the ITIL standards.

6.2.2. Specific Requirements for 'Platform as a Service' (PaaS)

The below mandatory requirements are applicable for services offered by CSP under Platform as a Service, using Government Community Cloud or Virtual Private Cloud or Public Cloud. These are in addition to the General Requirements for all Cloud Deployment Models and all Cloud Services Model.

The CSPs shall be responsible for all activities, roles, and responsibilities for services being offered using Platform as a Service as defined in Figure-1 of this document.

1. CSPs shall be responsible for monitoring and management of the PaaS platform.

2. CSPs shall ensure multiple range of runtime environments are supported to enable User Departments to choose the most appropriate technology for the task.

3. CSPs shall ensure that any services offered from Platform as a Service are portable and vertically integrated.

4. CSPs shall ensure that services offered from Platform as a Service are available with automatic scale up (adding more resources to handle demand) and scale out (adding more systems to handle demand) to meet User Department's performance requirements.

5. CSPs shall ensure that any service offered from Platform as a Service have 99.50 % UPTIME and there is no compromise on performance of the application.

6. CSPs shall be responsible to clearly demonstrate to MeitY / STQC or any 3rd party assessor appointed by STQC at the time of getting its services empaneled the mechanism for porting data into and out of the PaaS solution.

7. CSPs shall ensure that User Departments are provided with Central web-based tool for monitoring and management of services.

6.2.3. Specific Requirements for 'Software as a Service' (SaaS)

The below mandatory requirements are applicable for services offered by CSP under Software as a Service, using Government Community Cloud or Virtual Private Cloud or Public Cloud. These are in addition to the General Requirements for all Cloud Deployment Models and all Cloud Services Model.

The CSPs shall be responsible for all activities, roles, and responsibilities for services being offered using Software as a Service as defined in Figure-1 of this document.

1. Cloud services under SaaS model shall only be offered from Data Centers audited and qualified by STQC under the Cloud Services Empanelment process.

2. CSPs shall be responsible for ensuring that all data functions and processing are performed within the boundaries of India.

3. CSPs shall be responsible to ensure that the services offered from SaaS provide a mechanism to authenticate and authorize users.

4. SaaS solution / services offered to User Departments shall have in-built functionality to integrate with existing authentication mechanisms like Active-Directory.

5. SaaS solution shall be able to segregate users on basis of privileges granted to the users.

6. CSPs shall provision and implement role-based authentication when required and separation of identities shall be maintained in multi-tenant environment.

7. CSPs shall ensure that all the policies and procedures shall be established and maintained in support of data security to include confidentiality, integrity, and availability across various system interfaces and business functions to prevent any improper disclosure, alternation, or destruction.

8. CSPs shall ensure that any service offered as SaaS are monitored, controlled and administered using web-based tool with visibility to the User Department.

9. CSPs shall ensure that User Departments are provided with capability to generate custom reports around several parameters such as users, time, data, etc.

10. CSPs shall be responsible to provide a mechanism to enable each User Department's administrator to create, manage and delete user accounts for that tenant in the user account directory.

11. CSPs shall ensure that services offered under SaaS are available with automatic scale up (adding more resources to handle demand) and scale out (adding more systems to handle demand) to meet User Department's performance requirements.

12. CSPs shall ensure that any service offered from the SaaS solution provider comply with PII data security standards like ISO 27018:2019.

13. CSPs shall ensure that services offered under SaaS are enabled with data loss prevention tools and capability to monitor data flow.

14. CSPs shall ensure that services offered under SaaS provide tools / capability for encryption of data-at-rest, data-in-processing and data-in-transit.

15. CSPs shall ensure that services offered under SaaS support encryption algorithms like AES256 and higher.

6.2.4. General Requirements for all Cloud Service Models

The below requirements shall be applicable on all the Cloud services offered from any of the Cloud services model, i.e. Infrastructure as a Service, Platform as a Service, Software as a Service, offered using Public Cloud, Virtual Private Cloud and Government Community Cloud

a) Service Management and Provisioning Requirements

The below mandatory requirements are applicable for services offered from all Cloud Service Models, using any of the Cloud Deployment Models.

The CSPs shall ensure below mentioned requirements while provisioning the Cloud solution for the User Department are met.

1. Provisioning of virtual machines, storage and bandwidth dynamically (or on-demand) on a self-service mode or as requested.

2. Enable Service Provisioning via Application Programming Interface (API).

3. Secure provisioning, de-provisioning and administering [such as Secure Sockets Layer (SSL)/Transport Layer Security (TLS) or Secure Shell (SSH)]

4. Support the terms of service requirement of terminating the service at any time (on-demand).

5. Portal provisioned for the User Departments by the CSPs shall also contain the following information:

    a. Service Level Agreements (SLAs)

    b. Help Desk and Technical Support

    c. Resources (Technical Documentation, Articles/Tutorials, etc.)

6. The CSPs shall carry out the capacity planning and do the Infrastructure sizing for the User Department to identify & provision, where necessary, the additional capacity to meet the user growth and / or the peak load requirements to support the scalability and performance requirements of the solution. There should not be any constraints on the services.

7. The CSPs shall ensure that the effective Remote Management features exist so that issues are addressed by the CSPs in a timely and effective manner.

8. Service Provisioning shall be available with two-factor / multi factor authentication via the SSL through a web browser.

b) Operational Management

1. The CSPs shall ensure that technology refresh cycles are conducted from time to time to meet the performance requirements and SLAs. The management of network, storage, server, and virtualization layers, platforms as included by CSPs as part of their service offerings etc. shall be complete responsibility of CSPs during the technology refresh cycle.

2. The CSPs shall provide a secure, dual factor / multi-factor method of remote access which allows the Government Department designated personnel (privileged users) the ability to perform duties on the hosted infrastructure.

3. The CSPs shall ensure that hardware is upgraded periodically without any financial impact to the Government Department(s).

4. The applications / data hosted within the CSP environment shall be immediately deleted/destroyed and certify the VM and data destruction to the Government Department as per stipulations and shall ensure that the data cannot be forensically recovered.

5. CSPs shall ensure that patch management is performed from time to time or as & when required. CSPs shall alert the User Department in advance of any installation of patches via e-mail and cloud portal.

6. Patch management for OS security patches shall be responsibility of the CSP.

7. CSPs shall ensure that all OS images created within the Cloud platform are regularly patched with the latest security updates.

8. CSPs shall monitor availability of the servers, system software's and its network.

9. CSPs shall investigate outages, perform appropriate corrective action to restore the hardware, software, operating system, and related tools.

10. CSPs shall ensure that technology and hardware upgrades of their IT Infrastructure are done before end of product life cycle and warranty.
11. CSPs shall ensure that the software required by the User Department are provided with latest version. However, if required by the User Department, the operating system and database may be provisioned with not more than two version old.

c) Data Management

1. CSPs shall enforce security controls and policies to secure data from unauthorized access in a multi-tenant environment

2. CSPs shall provide tools and mechanisms to the Government Department or its appointed agency for defining its backup requirements & policy. The backup policy which is defined and implemented shall be an automated process and backups should be taken on different mediums.

3. The CSPs shall provide tools and mechanisms to the Government Department or its appointed agency for configuring, scheduling, performing and managing back-ups and restore activities (when required) of all the data including but not limited to files, folders, images, system state, databases and enterprise applications in an encrypted manner as per the defined policy.

4. CSPs shall be liable to transfer data back in-house or any other Cloud / physical environment as required by the User Department, either on demand or in case of contract or order termination for any reason.

5. CSP shall not delete any data at the end of the agreement (for a maximum of 45 days beyond the expiry of the Agreement) without the express approval of the Government Department.

6. CSPs shall ensure minimum 128-bit encryption is used for handling data at rest and in transit.

7. The CSPs shall be responsible for deleting or otherwise securing Government Department's Content/Data prior to VM deletion and in case deleted, shall ensure that the data cannot be forensically recovered when the Government Department or CSP (with prior approval of the Government Department) scales down the services.

d) User/Admin Portal Requirements

The CSP shall be responsible to meet the below requirements:

1. Utilization Monitoring

a. Provide automatic monitoring of resource utilization and other events such as failure of service, degraded service, etc. via service dashboard or other electronic means.

b. Real time performance thresholds

c. Real time performance health checks

d. Real time performance monitoring & Alerts

e. Historical Performance Monitoring

f. Capacity Utilization statistics

g. Cloud Resource Usage including increase / decrease in resources used during auto-scale

2. Incident Management

a. Provide Incident Management and Ticketing via web-based portal (tools) for any incident occurrence during the operations.

b. CSPs shall follow and adhere to latest ITIL V3 guidelines and process for the Incident management and Problem management.

c. CSPs shall provide a mechanism to carry out regular health check on Department provisioned cloud infrastructure and facilitate download of the health check report as per the frequency identified/set by the User Department.

d. For all Incidents / Issues with Severity 'Critical and High', the CSPs Incident Management Team shall be activated to provide resolution as per defined SLA's by the User Department and closure of the Incident. The teams shall be responsible to send an Incident Report on daily basis or as desired by User Department for all such Incidents to all the stake holders including designated officials by the department.

e. For any re-occurring issue, the Problem Management Process shall be initiated, and problem ticket shall be created for the same. After permanent resolution of the re-occurring issue / Problem, the Problem Ticket report should be sent across to all the stake holders.

3. User Profile Management

a. Support maintenance of user profiles

b. CRUD Operations (CREATE, READ, UPDATE, DELETE)

e) Integration Requirements

Provide support to all Application Programming Interfaces (APIs) including REST API that CSP develops/provides.

f) LAN / WAN Requirements

1. The CSPs shall ensure that Local Area Network (LAN) does not impede data transmission.
2. Provide a redundant local area network (LAN) infrastructure and static IP addresses from customer IP pool or "private" non-internet routable addresses from CSP pool.
3. Ability to deploy VMs in multiple security zones as required for the project, defined by network isolation layers in the Customer's local network topology.
4. Provide access to Wide Area Network (WAN).
5. Provide private connectivity between a Government Department's network and Data Center Facilities.
6. IP Addressing:
    - Provide IP address assignment, including Dynamic Host Configuration Protocol (DHCP).
    - Provide IP address and IP port assignment on external network interfaces.
    - Provide dedicated virtual private network (VPN) connectivity.
7. Provide infrastructure that is IPv6 compliant.
8. CSPs shall support for providing secure connection to the Data Center and Disaster Recovery Center (where applicable) from the Government Department Offices.
9. The data center and disaster recovery center facilities (where applicable) should support connection to the wide area network through high bandwidth links of appropriate capacity to take care of the needs of various types of user entities. Provision has to be made for segregation of access path among various user categories.
10. Support dedicated link to the offices of Government Departments to access the data center and a separate internet link for other external stakeholders to get access to Government Department services.
11. CSPs shall have the capability to provide adequate bandwidth between Primary Data Center and Disaster Recovery Center for data replication.
12. Support network level redundancy through MPLS lines from two different service providers, alternate routing paths facilitated at ISP backbone (MPLS), redundant network devices etc. These two network service providers should not share same back end infrastructure. Redundancy in security and load balancers, in high availability mode will be provided to facilitate alternate paths in the network.

g) Backup Services

1. The CSPs shall configure, schedule and manage backups of all the data including but not limited to files, folders, images, system state, databases and enterprise applications as per the policy defined by MeitY or the Government Department.

2. The CSPs shall be responsible for file system and database backup and restore services.

3. The CSPs shall be responsible for back up of virtual machines, storage volumes, file systems, and databases within the CSP's own Cloud environment.

4. The CSPs shall be responsible for monitoring, reporting, notifications/alerts & incident management, backup storage, scheduling & retention, restoration, backup data protection, etc.

5. The backup solution shall support retention period of minimum 30 days or as desired by the User Department as per their needs.

6. The backup solution offered by CSPs shall support granular recovery of virtual machines, database servers, Active Directory including AD objects, etc. Government Organization should be able to recover individual files, complete folders, entire drive, or complete system to source machine or any other machine available in network.

7. The backup service must provide following capabilities:

    - Compression: Support compression of data at source before backup
    - Encryption: Support at least 128-bit encryption at source
    - Alert: Support email notification on backup job's success / failure
    - File exclusion: Ability to exclude specific files, folders or file extensions from backup
    - Deduplication: Provide deduplication capabilities

h) Data Center Facilities Requirements

1. The data center facilities shall cater for the space, power, physical infrastructure (hardware).

2. The data center facilities and the physical and virtual hardware should be located within India.

3. The space allocated for hosting the infrastructure in the Data Center should be secure.

4. The Data Center should be certified with the latest version of ISO 27001 (year 2013) and provide service assurance and effectiveness of Management.

5. The NOC and SOC facility must be within India for the Cloud Environments and the managed services quality should be certified for ISO 20000-1:2018.

6. For any Government body / organization which shall avail Cloud services under this empanelment process, the CSPs shall be required to provide complete access of the IT Infrastructure to CERT-In. MeitY or any designated body selected by MeitY / User Department shall be able to carry out SOC and NOC operations for the MeitY empaneled services.

7. The Data Center should conform to at least Tier III standard (preferably certified under TIA 942 or Uptime Institute certifications by a 3rd party) and implement tool-based processes based on ITIL standards.

8. All the physical, environmental and security features, compliances and controls of the Data Center facilities (as required under this application document) shall be enabled for the environment used for offering Cloud services.

9. Provide staff (technical and supervisory) in sufficient numbers to operate and manage the functioning of the DC & DR with desired service levels.

10. The data center should comply with the Physical Security Standards as per ISO 27001:2013 standards.

11. CSPs shall be required to provide complete access of the Cloud Services to User Department or any designated body authorized by the User Department to carry out SOC and NOC operations.

12. The Applicant has to provide an undertaking on data center service arrangements as per Annexure - 11.

i) Cloud Storage Service Requirements

1. The CSPs shall ensure that the cloud storage services are made available online, on-demand, and dynamically scalable up or down as per request from the end users (Government Department or Government Department's nominated agencies) with two-factor authentication via the SSL through a web browser.

2. The CSPs shall provide scalable, redundant and dynamic storage facility.

3. The CSPs shall provide users with the ability to add / remove storage with two-factor authentication via the SSL through Cloud management portal and manage storage capabilities remotely via the SSL VPN clients as against the public internet.

j) Disaster Recovery & Business Continuity Requirements

1. CSP is responsible for Disaster Recovery Services so as to ensure continuity of operations in the event of failure of primary data center of the Government Department and meet the RPO and RTO requirements.

a. RPO should be less than or equal to 2 hours

b. RTO shall be less than or equal to 4 hours

c. Key transaction data shall have RPO of 15 minutes.

However, the User Department may seek more stringent RTO, RPO, or any other disaster recovery requirements as per their needs.

2. During the change from Primary DC to DR or vice-versa (regular planned changes), there should be minimal/no data loss depending on application requirements of the User Department.

3. There shall be asynchronous replication of data between Primary DC and DR and the CSP will be responsible for sizing and providing the DC-DR replication link so as to meet RTO and RPO requirements.

4. The DC & DR sites shall be separated by a minimum distance of 100 kilometers.

5. Replication Link sizing and provisioning shall be in scope of the CSP.

6. During normal operations, the Primary Cloud Data Center shall serve the requests. The Disaster Recovery Site will not be performing any work but will remain on standby. During this period, the compute environment for the application in DR shall be available on demand basis for a functional DR and minimum compute if required, as per the solution offered by the CSP or as desired by the User Department. The application environment shall be installed and ready for use.

7. In the event of a site failover or switchover, DR site shall take over the active role, and all the requests shall be routed through that site. Application data and application states shall be replicated between data centers so that when an outage occurs, failover to the surviving data center can be accomplished within the specified RTO. The compute environment for the application shall be equivalent to DC during this period.

8. The installed application instance and the database shall be usable, and the same SLAs as DC shall be provided. The use of this Full Compute DR environment can be for specific periods during a year for the purposes of DC failure or DR Drills or DC maintenance.

9. The security provisioned by CSP shall be for full infrastructure i.e. Cloud-DC and Cloud-DR.

10. The CSPs shall conduct DR drill once in every six months, of operation wherein the Primary DC shall be deactivated, and complete operations shall be carried out from the DR Site. However, during the change from DC to DR-Cloud or vice-versa (or regular planned changes), there should be no/minimal data loss depending on the application requirements of the user department.

11. The CSPs shall clearly define the procedure for announcing DR based on the proposed DR solution. The CSPs shall also clearly specify the situations in which disaster shall be announced along with the implications of disaster and the period required for migrating to DR. The CSPs shall plan all the activities to be carried out during the Disaster Drill and issue a notice to the User Department at least 15 working days before such drill.

12. RPO monitoring, Reporting and Events Analytics for the Disaster recovery solutions should be offered as part of the offering.

13. Any lag in data replication should be clearly visible in dashboard and its alerts should be sent to respective authorities.

14. The CSPs shall provide the solution document of DR to the User Department availing DR services.

15. The CSPs shall have proper escalation procedure and emergency response in case of failure/disaster at DC.

16. The CSPs shall demonstrate the DR site to run on hundred percent capacity for proving successful implementation of the DR site.

17. Automated switchover/failover facilities (during DC failure & DR Drills) to be provided and ensured by the CSP. The switchback mechanism shall also be automated process and no /minimal data loss depending upon application requirement of the User Department.

k) Security Requirements

1. The CSPs shall be responsible for provisioning, securing, monitoring and maintaining the hardware, network(s), and software that supports the infrastructure and present Virtual Machines (VMs) and IT resources to the Government Department..

2. The Data Center Facility of the CSP shall at minimum implement the security toolset: Security & Data Privacy (Data & Network Security including Anti-Virus, Virtual Firewall, Multi Factor Authentication, VPN, IPS, Log Analyzer / Syslog, SSL, DDoS Protection, HIDS / NIDS, Rights Management, SIEM, Integrated Vulnerability Assessment, SOC, Private Virtual Zones, Data Privacy, Data Encryption, Certifications & Compliance, Authentication & Authorization, and Auditing & Accounting)

3. The CSPs shall ensure that they meet the ever-evolving security requirements as specified by CERT-In (http://www.cert-in.org.in/).

4. The CSPs shall ensure that they comply to Cloud Security ISO Standard ISO 27017:2015 and Privacy Standard ISO 27018:2019.

5. Meet any security requirements published (or to be published) by MeitY or any standards body setup / recognized by Government of India from time to time and notified to the CSP by MeitY as a mandatory standard.

6. MeitY and Government Department reserves the right to verify the security test results. In case of the Government Community Cloud, MeitY and Government Department reserves the right to verify the infrastructure.

7. Implement industry standard storage strategies and controls for securing data in the Storage Area Network so that clients are restricted to their allocated storage.

8. Ability to create non-production environments and segregate (in a different VLAN) non-production environments from the production environment such that the users of the environments are in separate networks.

9. Cloud Offerings should have built-in user-level controls and administrator logs for transparency and audit control.

10. Cloud Platform should be protected by fully-managed Intrusion detection system using signature, protocol, and anomaly-based inspection, thus providing network intrusion detection monitoring.

11. Cloud Platform should provide Edge-to-Edge security, visibility and carrier-class threat management and remediation against security hazards like Denial of Service (DoS) and Distributed Denial of Service (DDoS) attacks, botnets, etc. Also, shall provide protection against network issues such as traffic and routing instability.

12. Cloud Platform should provide Web Application Filter for OWASP Top 10 protection as a service that can be enabled for Government Departments that require such a service.

13. Access to Government Department provisioned servers on the Cloud should be through SSL VPN clients only as against the public internet.

14. CSPs shall allow audits of all administrator activities performed by Government Department and allow Government Department to download copies of these logs in CSV or any other desired format.

15. Maintain the security features described below, investigate incidents detected, undertake corrective action, and report to Government Department, as appropriate.

16. CSPs shall deploy and update commercial anti-malware tools (for systems using Microsoft operating systems), investigate incidents, and undertake remedial action necessary to restore servers and operating systems to operation.

17. CSPs shall provide consolidated view of the availability, integrity and consistency of the Web/App/DB tiers.

18. CSPs shall ensure that password policies adhere to security requirements as defined by CERT-IN.

19. CSPs shall ensure that all GoI IT Security standards, policies, and reporting requirements are met.

20. CSPs shall meet and comply with all GoI IT Security Policies and all applicable GoI standards and guidelines, other Government-wide laws and regulations for protection and security of Information Technology.

21. CSPs shall generally and substantially and in good faith follow GoI guidelines and CERT-In and MeitY Security guidance. Where there are no procedural guides, generally accepted industry best practices for IT security shall be used by the CSPs.

22. Information systems must be assessed whenever there is a significant change to the system's security posture.

23. MeitY or MeitY appointed 3rd party shall conduct regular independent third-party assessments of the CSP's security controls to determine the extent to which security controls are implemented correctly, operating as intended and producing the desired outcome with respect to meeting security requirements and submit the results to MeitY and User Department.

24. In case CSP has industry standard certifications (assessed by a Third Party Auditor) that verify compliance against the security requirements of the application document, SLA & MSA, results, relevant reports, certifications may be provided with evidence along with the mapping of the industry standard certification controls against the application document requirements. However, if there are any requirements that do not fall under the industry standard certifications, the CSP shall get the Third Party Auditor to assess the conformance to the requirements.

25. MeitY reserves the right to perform Penetration Test. If MeitY exercises this right, the CSP shall allow MeitY's designated third party auditors to conduct activities to include control reviews that include but are not limited to operating system vulnerability scanning, web application scanning and database scanning of applicable systems that support the processing, transportation, storage, or security of Department's information. This includes the general support system infrastructure.

26. CSPs shall ensure that Identified gaps are tracked for mitigation in a Plan of Action document.

27. CSPs shall be responsible for mitigating all security risks found and continuous monitoring activities. All high-risk vulnerabilities must be mitigated within 30 days and all moderate risk vulnerabilities must be mitigated within 90 days from the date vulnerabilities are formally identified. The Government will determine the risk rating of vulnerabilities.

28. CSPs shall provide access to MeitY or their designee acting as their agent when requested, in order to verify compliance with the requirements for an Information Technology security program. MeitY reserves the right to conduct on-site inspections. CSPs shall make appropriate personnel available for interviews and documentation during this review. If the documentation is considered proprietary or sensitive, these documents may be reviewed on-site under the CSP's supervision.

29. CSPs shall provide vulnerability scan reports from Web Application, Database, and Operating System Scans or the services for the Government Department to run the vulnerability scan. The scan results (that fall under the scope of the CSP) shall be managed and recorded in Plans of Action and mitigated by the CSP.

30. All documents exclusively produced for the project are the property of the Government Department and cannot be reproduced or retained by the CSP. All appropriate project documentation will be given to Government Department during and at the end of this contract or at the time of termination of the contract. The CSP shall not release any project information without the written consent of the Government Department. Any request for information relating to the Project presented to the CSP must be submitted to the Government Department for approval.

31. CSPs shall protect all Government Department data, equipment, etc. by treating the information as sensitive. Sensitive but unclassified information, data, and/or equipment shall only be disclosed to empaneled-personnel from the User Department. CSPs shall keep the information confidential, use appropriate safeguards to maintain its security in accordance with minimum standards. When no longer required, this information, data, and/or equipment shall be returned to Government Department control, destroyed, or held until otherwise directed by the Government Department. CSPs shall destroy unneeded items by burning, shredding, or any other method that precludes the reconstruction of the material.

32. MeitY has the right to perform manual or automated audits, scans, reviews or other inspections of the CSP's IT environment being used to provide or facilitate services for the User Departments through a MeitY's designated third party auditor. CSPs shall be responsible for the following privacy and security safeguards.

33. CSPs shall not publish or disclose in any manner, without MeitY's written consent, the details of any safeguards either designed or developed by the CSPs under the Agreement or otherwise provided by the GoI& Government Department.

34. To the extent required to carry out a program of inspection to safeguard against threats and hazards to the security, integrity, and confidentiality of any non-public Government data collected and stored by the CSP, the CSP shall allow MeitY logical and physical access to the CSP's facilities, installations, technical capabilities, operations, documentation, records, and databases within 72 hours of the request. Automated audits shall include but are not limited to the following methods:

i. Authenticated and unauthenticated operating system/network vulnerability scans

ii. Authenticated and unauthenticated web application vulnerability scans

iii. Authenticated and unauthenticated database application vulnerability scans

35. Automated scans shall be performed by MeitY's designated third party auditors using MeitY specified tools. If the CSP chooses to run its own automated scans or audits, results from these scans may, at MeitY's discretion, be accepted in lieu of MeitY performed vulnerability scans. In these cases, scanning tools and their configuration shall be approved by MeitY. In addition, the results of CSP-conducted scans shall be provided in full to MeitY.

36. Submission to regular audits: CSPs shall submit documents as desired for regular audits commissioned by MeitY. The purpose of these audits shall not only be to ensure conformance with the requirements stated in this application document, but also to ensure that the implementation is executed in the best of ways to meet the requirements of MeitY. These audits may be conducted by MeitY or MeitY's designated third party auditors. CSP will cooperate fully with the auditor. MeitY will inform the CSP of the short-comings if any after the audit is completed and the CSP will respond appropriately and address the identified gaps.

37. For compliance to the government regulations, it is required that Cloud services offered shall be hosted within India and data residency shall also be limited to the boundaries of India.

38. All data functions and processing shall be performed within the boundaries of India.

39. No data, whether in the form of backups or otherwise should be transmitted outside the boundaries and legal jurisdiction of India.

40. CSPs shall have capability / feature to define strong password policy and maintaining password complexity rules and shall also include the prohibition of changing of password/PIN lengths and any authentication requirements.

41. CSPs shall also make sure that copy of customer data will be provided in the standard format to maintain portability.

42. CSPs shall ensure that all the policies and procedures shall be established with supporting business processes and technical measures implemented for the secure disposal and complete removal of data from all storage media, ensuring data is not recoverable by any computer forensic means.

43. CSPs shall ensure that all the policies and procedures are established and supporting processes and technical measures are implemented for timely detection of vulnerabilities within organizationally-owned or managed applications, infrastructure network and system components (e.g., network vulnerability assessment, penetration testing) to ensure the efficiency of implemented security controls.

l) Legal Compliance Requirements

The CSPs shall be liable to comply with all the legal requirements defined by MeitY.

1. IT Act 2000 (including 43A) and amendments thereof.
2. Meet the ever-evolving security requirements as specified by CERT-In (http://www.cert-in.org.in/).
3. Meet any security requirements published (or to be published) by MeitY or any standards body setup / recognized by Government of India from time to time and notified to the CSP by MeitY as a mandatory standard.
4. All services acquired under this application document including data will be guaranteed to reside in India only.
5. There shall not be any legal frameworks outside Indian Law applicable to the operation of the service (and therefore the information contained within it).
6. A copy of the contract / MOU (excluding the commercials) between CSP & Government Department for the purpose of the project, aligned to the terms & conditions of the application document should be provided to MeitY, as and when requested by MeitY.
7. MeitY has initiated the process of identification of the standards, develop the necessary specifications, frameworks and guidelines including the guidelines for empanelment of Cloud Service Offerings. The guidelines may also include continuous monitoring of the shared systems that can be leveraged by Government to both reduce their security compliance burden and provide them highly effective security services.
8. The empaneled Cloud services shall have to comply with the guidelines & standards as and when such guidelines / standards are published by MeitY within the timeframe given by MeitY.
9. CSPs shall be prepared to submit the necessary artifacts and independent verification within the timeframe determined by MeitY once the guidelines & standards are published by MeitY.
10. CSPs shall be responsible for all costs associated with implementing, meeting, assessing, documenting and maintaining the registration.
11. The cost of meeting all requirements, maintaining empanelment of it's Cloud Service Offering shall be the responsibility of CSP.
12. If the CSP fails to meet the guidelines & standards as set by GoI within the timeframe set by MeitY, the Government Department reserves the right to terminate the contract and request to move to a different CSP that meets the mandatory guidelines & standards at no additional

cost to Government Department. The Exit Management provisions shall come into effect in such a scenario.

13. CSPs shall be responsible for the following privacy and security safeguards:

    a. CSPs shall not publish or disclose in any manner, without the Government Department's written consent, the details of any safeguards either designed or developed by the CSP under the agreement or otherwise provided by the Government Department or Government of India.

    b. CSPs shall adhere to the privacy safeguards as laid down by the MeitY and Government Department.

    c. To the extent required to carry out a program of inspection to safeguard against threats and hazards to security, integrity and confidentiality of any non-public Government data collected and stored by the CSP, the CSP shall afford the MeitY or its nominated agency access to the CSP's facilities, installations, technical capabilities, operations, documentation, records, and databases.

    d. If new or unanticipated threats or hazards are discovered by either MeitY or Government Department, Government or the CSP, or if existing safeguards have ceased to function, the discoverer shall immediately bring the situation to the attention of CERT-In and the other party.

    e. CSPs need to adhere to the guidelines and acts published by Government of India. No data should be shared to any third party without explicit approval by the User Department, unless legally required to do so by court of law in India.

14. The empaneled Cloud services shall have to comply with the guidelines & standards as and when published by Govt. of India. CSPs shall be responsible for all costs associated with implementing, assessing, documenting and maintaining the empanelment and any guidelines published by MeitY shall be followed by the CSPs.

15. In case any misconduct is found, MeitY / User Department reserves the right to take appropriate legal course of action including blacklisting of the CSP.

m)Management Reporting Requirements

The CSPs shall ensure deliverables listed below should be accessible via online interface not later than 10 days after the end of the calendar month and available for up to one year after creation. The information shall be available in format approved by MeitY / User Department. The CSPs shall monitor and maintain the stated service levels as agreed in the Service Level Agreement between the Government Department and the CSP. CSPs shall provide regular monthly reports to MeitY. In addition to this, MeitY reserves the right to seek any additional reports based on specific issues / concerns with respect to provisioning or availing Cloud services.

Cloud Service Providers shall also provision real time dashboard for monitoring and reporting purposes for MeitY.

1. Service Level Management
    a. Service Level Management Reports (as per the service levels agreed in the Service Level Agreement between the Government Department and the CSP).
    b. Service Availability at the VM & Service Availability at the Storage Level (Measured as Total Uptime Hours / Total Hours within the Month) displayed as a percentage of availability up to one-tenth of a percent (e.g. 99.5%).
    c. Text description of major outages (including description of root-cause and fix) resulting in greater than 1-hour of unscheduled downtime within a month.
2. Network and Security Administration (including security breaches with classification, action taken by the CSP and current status) related reports.
3. Help Desk / Trouble Tickets raised by the MeitY and / or Government Department.
4. Number of Help Desk/customer service requests received.
5. Number of Trouble Tickets Opened.
6. Number of trouble tickets closed.
7. Average mean time to respond to Trouble Tickets (time between trouble ticket opened and the first contact with customer).
8. Average mean time to resolve trouble ticket.
9. Monthly utilization (including peak and non-peak volumetric details) of the Service Offerings for the respective Government Department.
10. Centralized Monitoring & Management and Reporting with:
    a. Alerts on event threshold and policy-based actions upon deviations.
    b. Internet & Intranet Data Transfer.
    c. Virtual Instances (vCPU, vMemory, Storage and Network Port) configuration and utilization.
    d. Storage Volume (Read/Write and IOPS)
    e. Load balancer
    f. Application Services

g. Database Monitoring

h. Reports on non-conformance and escalation for privileged access by unpaneled roles/ identities.

11. Government / User Departments shall have ten (10) business days to review, accept or reject all deliverables. Any comments made by the Government Department shall be addressed and a revised deliverable submitted within five (5) business days after the receipt of the comments/rejection, unless a further time extension for incorporating the comments is approved by Government Department.

12. The CSPs shall be responsible for third party audits certification (at the cost of CSP) every six months indicating the conformance to the requirements detailed in this application document of the empanelment of Cloud services which are being used by the Government Department. In case the empaneled Cloud services are not deployed for any Government Department, a self-certification every six months indicating the conformance to the requirements detailed in this application document, SLA & MSA of the environments & Cloud Service Offerings empaneled should be provided to MeitY.

13. CSPs shall provide regular monthly reports having at least the following information about the User Department procuring the Cloud services, Name of the Cloud services, Cloud Deployment Model (s) selected, Cloud Service Model (s) selected, Month & Year of Award of Work Order) to MeitY as per the report template shared by MeitY.

n) Service Level Agreement Management

1. Provide a robust, fault tolerant infrastructure with enterprise grade SLAs with an assured uptime of 99.5%, SLA measured at the VM Level & SLA measured at the Storage Levels.

2. Service Availability (Measured as Total Uptime Hours / Total Hours within the Month) displayed as a percentage of availability up to one-tenth of a percent (e.g. 99.5%).

3. Within a month of a major outage occurrence resulting in greater than 1-hour of unscheduled downtime. Describe the outage including description of root-cause and fix.

4. Service provisioning and de-provisioning times (scale up and down) in near real- time should be as per the SLA requirement of the Government Department. The provisioning / de-provisioning SLAs may differ for the different Cloud Deployment Models.

5. Helpdesk and Technical support services to include system maintenance windows.

6. CSPs shall implement the monitoring system including any additional tools required for measuring and monitoring each of the Service Levels as per the SLA between the Government Department and the CSP.

6.3. Compliance Requirements

CSPs are required to show their compliances to the requirements specified in Annexure 13. It is mandatory that all certifications requested as part of the application shall be issued in the name of the CSP as per the table given below.

Certification	Issued in the name of
ISO 27001 :2013	CSP
ISO 20000-1:2018	CSP
ISO 27017:2015	CSP
ISO 27018:2019	CSP
TIA-942 / UPTIME (Tier III or higher)	CSP/Data Center Facility Owner

The CSP willing to get its services empaneled shall be fully responsible to submit all the required certificates and documents to MeitY / STQC.

7. Governance Structure and Roles of the Different Agencies

MeitY is the authorized department in Government of India with regards to empanelment of the Cloud Service Offerings of the service providers. To monitor the compliance on an on-going basis and address any non-compliances or deviations from the requirements, MeitY will form a suitable Governance mechanism.

Roles and Responsibilities of MeitY or an Agency nominated by MeitY

1. Primary owner of the Empanelment Process
2. Empanelment of the Cloud Service Offering of the Cloud Service Provider
3. Setup of GI Cloud Services Directory
4. Publish empaneled Cloud Service Offerings on the GI Cloud Services Directory
5. Monitoring and ensuring compliance to the empanelment guidelines by the Cloud Service Providers
6. Review and Approve the new Data Center Facility (or Facilities) submitted by the service provider that are found compliant to the requirements of the Empanelment Application and any amendments thereof. The above is applicable once the Cloud Service Offerings of the service provider from the technically qualified (proposed at the time of the submission of Application) Data Center Facility (or facilities) are empaneled by MeitY and the service provider chooses to offer the empaneled Cloud Service Offerings from a different or additional Data Center Facility (or Facilities).
7. Setup the Governance Structure to review and approve changes / modifications of the deployed solution, database, data, configurations, security solutions, hosted infrastructure, etc. of the dedicated infrastructure and solutions of the Government Community Cloud where such changes affect solutions of multiple Government Departments using the Government Community Cloud.
8. There will be no payment to the Empaneled Cloud Service Providers from MeitY.
9. Roles and Responsibilities of Government Department
    a) Evaluate the suitability of applications / services / projects to leverage Cloud Services.
    b) Capacity Sizing to estimate compute, storage, and network requirements.
    c) Assessment of the risk and security profile of their application / data / services and identify the appropriate Cloud Deployment Model and Cloud service offering.

d) Select a Cloud Service (IaaS, PaaS, DRaaS,…) from the empaneled Cloud Service Offerings based on the requirements of the end User Department and considering the procurement guidelines, SLAs and MSA published by MeitY.

e) Enter into a Master Services Agreement and Service Level Agreement with the selected Cloud Service Provider / Managed Service Provider / System Integrator, aligned with the guidelines on Master Services Agreement and Service Level Agreement provided by MeitY.

f) Migrate to Cloud services with assistance from the Cloud Service Provider (or a Managed Service Provider or a System Integrator).

g) Management of Government Department's solution and relevant configurations on the Cloud infrastructure provided by the Cloud Service Provider.

h) Monitoring Service Level Agreement (SLAs) and other management reports provided by the Cloud Service Provider / Managed Service Provider / System Integrator.

i) Payment to the Cloud Service Provider / Managed Service Provider / System Integratorbased on the Service Level Agreement (SLA) and Master Services Agreement (MSA).

j) Review and approve changes / modifications to configurations specific to a Government Department.

10. Roles and Responsibilities of Cloud Service Provider

a) Comply on an on-going basis to the requirements specified under this Empanelment Application.

b) Comply on an on-going basis to the requirements specified under the application document, SLA and MSA with the Government Department.

c) Submit the details of the proposed Data Center Facility (or Facilities) including the compliance matrix against the relevant requirements for approval to MeitY. The above is applicable once the Cloud Service Offerings of the service provider from the technically qualified (proposed at the time of the Submission of Application) Data Center Facility (or facilities) are empaneled by MeitY and the service provider chooses to offer the empaneled Cloud Service Offerings from a different or additional Data Center Facility (or Facilities).

d) The CSPs may also authorize their Managed Service Providers for selling cloud services, as per the guidelines to be issued by GeM.

8. Instructions to Applicants

Availability of the Application Documents: The application/proposal can be downloaded from the website given underSection 3. The Applicants are expected to examine all instructions, forms, terms, project requirements and other information in this application document. Failure to furnish all information required as mentioned in the documents or submission of a proposal not substantially responsive to the requisite documents in every respect will be at the Applicant's risk and may result in rejection of the proposal and forfeiture of the EMD.

1. **Earnest Money Deposit (EMD):**

    a. Applicants shall submit an amount of INR 10 Lakhs (Rupees Ten Lakhs only), as Earnest Money Deposit ("EMD")

    b. EMD has to be in the form of a Bank Guarantee issued by any of the commercial banks in the format provided in the Annexure 14.

    c. EMD in any other form will not be accepted.

    d. EMD shall be valid for a period of 225 days from the last date of submission of the Application.

    e. The EMD of all unsuccessful applicants would be refunded by MeitY within three months of the applicant being notified by MeitY as being unsuccessful. The EMD of all the successful applicants would be refunded by MeitY within three months of the applicants acknowledging and accepting the Award of Empanelment by MeitY.

    f. No interest shall be payable by MeitY to the Applicant(s) on the EMD amount for the period of its currency.

    g. The application without adequate EMD, as mentioned above, will be liable for rejection without providing any further opportunity to the Applicant concerned.

    h. The applicant shall extend the validity of the EMD on request by MeitY

    i. The EMD may be forfeited:

        i. In case of a successful application, if the applicant fails to acknowledge and accept the Letter of Award of Empanelment from MeitY in accordance with terms and conditions

        ii. If the Applicant tries to influence the evaluation process

2. **Applicant inquiries and MeitY's responses:**

a. All enquiries from the Applicants relating to this application document must be submitted in writing exclusively to the contact person notified by MeitY in the format specified in Annexure - 12 'Request for Clarification Format'. A copy of the Applicant enquiries should also be emailed to the issuer's email address provided in the Section - 3. The mode of delivering written questions would be through post or email. In no event will MeitY be responsible for ensuring that Applicants' inquiries have been received by them. Telephone calls will not be accepted for clarifying the queries.

b. After the application document is issued to the Applicant, MeitY shall accept written questions/inquiries from the Applicants. MeitY will endeavour to provide a complete, accurate and timely response to all questions of all the Applicants. However, MeitY makes no representation or warranty as to the completeness or accuracy of any response, nor does MeitY undertake to answer all the queries that have been posed by the Applicants. All responses given by MeitY will be published on the website given under Section 3. In case the acknowledgement with the necessary details is submitted by the Applicant on receipt of the application document, MeitY may send the clarifications to such Applicants through e-mail. All responses given by MeitY will be available to all the Applicants. Any email communications sent by Applicants to MeitY must be sent to the email address provided in Section - 3.

3. Supplementary Information / Amendment to the Application Document

a. If MeitY deems it appropriate to revise any part of this application document or to issue additional data to clarify an interpretation of the provisions of this application document, it may issue supplements to this application document. Such supplemental information, including but not limited to, any additional conditions, clarifications, minutes of meeting, and official communication over email/post will be communicated to all the Applicants by publishing on the website given under Section - 3. In case the acknowledgement with the necessary details is submitted by the Applicant on receipt of the application document, MeitY may send the supplemental information / amendment to such Applicants through e-mail. Any such supplement shall be deemed to be incorporated by this reference into this application document.

b. The letters seeking clarifications sent either to all the Applicants or to specific Applicant as the case may be during the evaluation of technical proposal and the minutes of the meeting recorded during the technical evaluation shall also be deemed to be incorporated by this reference in this application document.

c. At any time prior to the deadline (or as extended by MeitY) for submission of applications, MeitY, for any reason, whether at its own initiative or in response to clarifications requested by prospective Applicant, may modify the application document by issuing amendment(s). All such amendments will be published on the website given under Section - 3. In case the acknowledgement with the necessary details is submitted by the Applicant on receipt of the application document, MeitY may send the

amendment(s) to such Applicants through e-mail. All such amendment(s) will be binding on all the Applicants.

d. In order to allow Applicants a reasonable time to take the amendment(s) into account in preparing their applications, MeitY, at its discretion may extend the deadline for the submission of applications.

4. **Application Preparation Costs:** The Applicant is responsible for all costs incurred in connection with participation in this process, including but not limited to, costs incurred in conduct of informative and other diligence activities, participation in meetings/discussions/presentations, preparation of proposal in providing any additional information required by MeitY to facilitate the evaluation process and all such activities related to the Application submission process. This Empanelment Application does not commit MeitY to award a contract or to engage in negotiations. Further, no reimbursable cost may be incurred in anticipation of award of the contract for implementation of the project.

5. **MeitY's right to terminate the process**

a. MeitY may terminate the application process at any time without assigning any reason. MeitY makes no commitments, explicit or implicit, that this process will result in a business transaction with anyone.

b. This application document does not constitute an offer by MeitY. The Applicant's participation in this process may result in MeitY selecting one or more Applicants to engage in further discussions and negotiations towards issue of Letter of Award of Empanelment. The commencement of such negotiations does not, however, signify a commitment by MeitY to execute a contract or to continue negotiations.

c. MeitY has the right to terminate this discussions and negotiations process without assigning any reason and no costs will be reimbursed to the participating Applicants.

d. MeitY reserves the right to reject any request for empanelment and to annul the empanelment process and reject all such requests at any time prior to empanelment, without thereby incurring any liability to the affected Applicant(s) or any obligation to inform the affected Applicant(s) of the grounds for such decision.

6. **Acceptance of part / whole application / modification – Rights thereof**: MeitY reserves the right to modify the technical specifications / quantities / requirements / tenure mentioned in this application document including addition / deletion of any of the item or part thereof after clarification provided by MeitY and the right to accept or reject wholly or partly application, or, without assigning any reason whatsoever. No correspondence in this regard shall be entertained. MeitY also reserves the unconditional right to place order wholly or partly to successful Applicant.

7. **Authentication of Applications:** The original and all copies of the application response shall be typed or written in indelible ink and signed by the Applicant or a person duly authorized to bind the Applicant to the Contract. A certified true copy of the corporate sanctions/approvals authorizing its authorized representative to sign/act/execute documents forming part of this proposal including various Application documents and binding contract shall accompany the application response. All pages of the application, except for un-amended printed literature, shall be initialed and stamped by the person or persons signing the Application.

8. **Interlineations in Application:** The Application shall contain no interlineations, erasures or overwriting except as necessary to correct errors made by the Applicant, in which case such corrections shall be initialed by the person or persons signing the application.

9. **Venue & Deadline for submission of Empanelment Application:**

a. Application, in its complete form in all respects as specified in the Empanelment application document, must be submitted to MeitY at the address specified in Section 3.

10. **Late Applications:** Applications received after the last date and the specified time (including the extended period if any) for any reason whatsoever, shall not be entertained and shall be returned unopened.

11. **Conditions under which this Application Document is issued:**

    a. This Application Form is not an offer and is issued with no commitment. MeitY reserves the right to disqualify any Applicant, should it be so necessary at any stage for any reason whatsoever.

    b. Timing and sequence of events resulting from this Application shall ultimately be determined by MeitY.

    c. No oral conversations or agreements with any official, agent, or employee of MeitY shall affect or modify any terms of this Application and any alleged oral agreement or arrangement made by an Applicant with any department, agency, official or employee of MeitY shall be superseded by the definitive agreement that results from this Application process. Oral communications by MeitY to Applicants shall not be considered binding on MeitY, nor shall any written materials provided by any person other than MeitY.

    d. Neither the Applicant nor any of the Applicant's representatives shall have any claims whatsoever against MeitY or any of their respective officials, agents, or employees arising out of, or relating to this Application or these procedures (other than those arising under a definitive service agreement with the Applicant in accordance with the terms thereof).

    e. The information contained in this document is only disclosed for the purposes of enabling Applicants to submit an application to MeitY. No part of this document

including the Annexure can be reproduced in any form or by any means, disclosed or distributed to any party not involved in the Application process without the prior consent of MeitY except to the extent required for submitting proposal. This document should not therefore be used for any other purpose.

12. **Rights to the Content of the Empanelment Application Response:** All the applications and accompanying documentation submitted as **Empanelment Application Response**against this Application will become the property of MeitY and will not be returned after opening of the pre-qualification response. If any Applicant does not qualify in pre-qualification stage, the technical response shall not be evaluated. MeitY is not restricted in its rights to use or disclose any or all of the information contained in the proposal and can do so without compensation to the Applicants. MeitY shall not be bound by any language in the proposal indicating the confidentiality of the proposal or any other restriction on its use or disclosure. MeitY has the right to use the services of external experts to evaluate the proposal by the Applicants and share the content of the proposal either partially or completely with the experts for evaluation with adequate protection of the confidentiality information of the Applicants.

13. **Modification and Withdrawal of Applications:** No application shall be modified or withdrawn in the intervening period between the deadline for submission of applications and the expiration of the validity period specified by the Applicant on the application form. Entire application security may be forfeited if any of the Applicants modify or withdraw their application during the validity period.

14. **Non-Conforming Application Response:** An Application Responsemay be construed as a non-conforming proposal and ineligible for consideration if:

    a. It does not comply with the requirements of this Application Document. Failure to comply with the technical requirements and failure to acknowledge the receipt of amendments, are common causes for holding proposals non-conforming.

    b. A proposal appears to be “canned” presentations of promotional materials that do not follow the format requested in this Application or do not appear to address the particular requirements given in the Application Document, and any such Applicants may also be disqualified.

15. **Disqualification:** The Application Response is liable to be disqualified in the following cases:

    a. Application Response submitted without EMD;

    b. Application Responsenot submitted in accordance with the procedure and formats prescribed in this document or treated as non-conforming proposal;

    c. The Applicant qualifies the proposal with its own conditions or assumptions;

d. Application Responseis received in incomplete form;

e. Application Responseis received after due date and time;

f. Application Responseis not accompanied by all the requisite documents;

g. Application Responseis not properly sealed or signed;

h. Information submitted in Application Responseis found to be misrepresented, incorrect or false, accidentally, unwittingly or otherwise, at any time during the processing of the contract (no matter at what stage) or during the tenure of the empanelment including the extension period of the empanelment period if any;

i. Applicant tries to influence the proposal evaluation process by unlawful/corrupt/fraudulent means at any point of time during the process;

j. In case one Applicant submits multiple Application Responsesor if common interests are found in two or more Applicants, the Applicants are likely to be disqualified;

k. Applicant fails to acknowledge and accept the Letter of Award of Empanelment within 30 working days from the date of notice of award or within such extended period, as may be specified by MeitY;

l. Applicants may specifically note that while evaluating the Application Responses, if it comes to MeitY's knowledge expressly or implied, that some Applicants may have colluded in any manner whatsoever or otherwise joined to form an alliance resulting in delaying the processing of proposal then the Applicants so involved are liable to be disqualified for this contract as well as for a further period of three years from participation in the empanelment process;

m. Applicants or any person acting on its behalf indulges in corrupt and fraudulent practices;

n. In case Applicant fails to meet any of the guidelines as indicated in this Empanelment Application;

o. The Applicants/authorized signatory is required to put the original signature, no scanned image of signature will be accepted, and the application will be rejected;

p. No redaction on the content/text of the documents is allowed, non-adherence to this will result in rejection of application.

16. **Acknowledgement of Understanding of Terms:** By submitting an Application Response, each Applicant shall be deemed to acknowledge that it has carefully read all sections of this Application Document, including all forms, schedules and annexure hereto, and has fully informed itself as to all existing conditions and limitations.

17. **Application Validity period:** The application should remain valid for a period of 180 days from the date of the submission of application. An application valid for a shorter period may be rejected as non-responsive. On completion of the validity period, unless the Applicant withdraws his proposal in writing, it will be deemed to be valid until such time that the Applicant formally (in writing) withdraws his application. In exceptional circumstances, at its discretion, MeitY may solicit the Applicant's consent for an extension of the validity period. The request and the responses thereto shall be made in writing or by fax or email.

18. **Language of Empanelment Application Response:** The application and all correspondence and documents shall be written in English.

19. **Application Response Submission Instructions:** The Application Response should be submitted as below:

    a. Pre-qualification Response - The format for submission of pre-qualification information is provided in Annexure - 6.

    b. Technical Response – The format for submission of technical requirement is provided in Annexure-7.

    c. The pre-qualification and the technical responses together with all supporting documents should be submitted in two separate sealed covers. Each cover should be clearly marked to indicate whether it contains pre-qualification response or technical response.

    d. The two envelopes mentioned above should be placed in a bigger envelope marked “Response to Empanelment Application of Cloud Service Offerings” together with the following:

        i. Covering Letter from the Applicant as per the format provided in Annexure-1.

        ii. An EMD as per details of provided under Clause (1) of Section 8.

        iii. A letter of authorization supported by Board Resolution/a power of attorney.

    e. All the envelopes shall have the name and address of the Applicant to enable the proposal to be returned unopened in case it is declared "late” or the proposal does not qualify.

    f. The Applicants are requested to sign across the envelopes along the line of sealing to ensure that any tampering with the response cover could be detected.

    g. The envelope containing the Empanelment Application Response should be delivered to MeitY by hand or by post at the address given in Section - 3 and date given inSection 4.

h. The pre-qualification response and technical response should be submitted in both Hardcopy and Softcopy forms in the format given in Annexure-6 and Annexure-7 respectively. The softcopy should be submitted in separate DVDs / USB drives, each for pre-qualification and technical response.

i. If any Applicant does not qualify in pre-qualification evaluation, the technical response shall not be evaluated.

j. Applicants are requested to submit a response that is to the point and refrain from providing unwanted information that is not relevant to this Application.

9. Process of Evaluation

1. Pre-Qualification Criteria

a. The Applicant will be assessed on the mandatory pre-qualification criteria specified under Annexure- 5, and the Applicant shall submit the information for pre-qualification in the form at Annexure- 6.

b. MeitY will assess the Applicant's capabilities against the pre-qualification criteria. Only those Applicants who meet / exceed the pre-qualification criteria shall proceed for technical evaluation.

i. Technical Evaluation Criteria

a. Applicants that satisfy the pre-qualification criteria will be considered for the Technical Evaluation.

b. The Committee shall evaluate the technical proposal to verify the compliance against the requirements in this Application Document. The Applicant shall submit the Technical Proposal in the form at Annexure-7.

2. Audit by STQC (or auditors empanelled by STQC)

a. Applicants that satisfy the pre-qualification and technical evaluation will be audited by STQC.

b. The Audit Guidelines and Process is as per the details published by MeitY/ STQC

3. Evaluation Process

a. The evaluation of the responses to the Application will be done by an Evaluation committee of MeitY.

b. MeitY may seek additional information and clarifications from any or all of the Applicants on the Pre-Qualification and Technical Responses submitted by the Applicant.

c. The evaluation shall be strictly based on the information and supporting documents provided by the Applicants in the application submitted by them. It is the responsibility of the Applicants to provide all supporting documents necessary to fulfill the mandatory eligibility criteria. In case, information required by MeitY is not provided by Applicant, MeitY may choose to proceed with evaluation based on information provided and shall not request the Applicant for further information. Hence, responsibility for providing information as required in this form lies solely with Applicant.

d. The Evaluation Committee shall first evaluate the Pre-Qualification Response as per the Pre-Qualification Criteria above. The Pre-Qualification Response shall be evaluated based on the information provided in the Form at Annexure-6 and the supporting documents submitted.

e. The technical response of only those Applicants who qualify in the evaluation of the pre-qualification stage shall be opened.

f. Each of the responses will be evaluated for compliance against the mandatory requirements in this Application Document. Only those Applicants who meet all the mandatory criteria and are found to be compliant against the requirements in this Application Document will be audited by STQC.

g. The results of the evaluation will be communicated to all the Applicants.

4. **Failure to agree with the Terms and Conditions of the Empanelment Application:** Failure of the successful Applicants to agree with the Terms & Conditions of the Applicationshall constitute sufficient grounds for the disqualification of the application.

5. Award of Empanelment

a. The Letter of Award of Empanelment will be issued by MeitY to the Applicants whose response conforms to the requirement of this document and are successfully audited by STQC, complying with the audit criteria.

b. MeitY will notify the successful Applicants in writing or by email, to be confirmed in writing by letter, that its application for empanelment has been accepted and will issue a Letter of Award of Empanelment.

c. MeitY will promptly notify each unsuccessful applicant and return their EMD

d. The successful Applicants should acknowledge and accept the Award of Empanelment by MeitY within 30 days of receipt of the letter of award in the prescribed format based on the terms and conditions contained in this Application Document.

6. **Empanelment:** The Cloud Service Providers whose service offerings are empaneled will be intimated by MeitY and have to acknowledge and accept the Letter of Award of Empanelment accepting the terms and conditions laid down in the application document. After agreeing to the Terms and Conditions, no variation or modification shall be made except by written amendment signed by both parties.

7. Empanelment Duration:

The empanelment window shall be opened for a period of two month from the date of release of application. Refer to Section 4 for detailed timelines on the application.

The empanelment shall be valid for a period of three years from the date of Award of empanelment.

Thereafter, each CSP shall also undergo a surveillance audit every year for the following two requirements.

(i) Minimum security requirements specified by MeitY

(ii) Any additional requirements specified by MeitY / requirements arising out of any additional service proposed to be offered by the CSP

8. Allocation of Work

a. The service provider shall not assign the project to any other agency, in whole or in part, to perform its obligation under the agreement.

b. This empanelment by MeitY does not guarantee allocation of work.

c. The Government Department may select from the empaneled Cloud Service Offerings of the service providers.

d. Empanelment with MeitY does not guarantee that any or all Applicants shall be awarded any project / assignment as a result of this empanelment.

9. New Data Center Facilities:

The below is applicable once the Cloud Service Offerings of the Cloud Service Provider from the technically qualified (proposed at the time of the Submission of Application) Data Center Facility (or facilities) are empaneled by MeitY and the service provider chooses to offer the empaneled Cloud Service Offerings from a different or additional Data Center Facility (or Facilities):

(i) The service provider is required to submit the details of the proposed Data Center Facility (or Facilities) indicating the compliance against the relevant requirements under the application document and any amendments thereof for approval to MeitY.

(ii) This addition of data center facility will be accepted through a fresh application and will follow the entire empanelment and audit process.

10. General Conditions

1. Applicant represents and warrants that it is in compliance with, and shall continue to comply with, all applicable laws, ordinances, rules, regulations, and lawful orders of public authorities of any jurisdiction in which work shall be performed under this Empanelment.

2. MeitY reserves the right to terminate the empanelment by giving a notice of one month if the performance of the Cloud Service Provider is not found satisfactory. The Cloud Service Providershall be given a period of thirty days to cure the breach or fulfil the empanelment obligations, failing which MeitY shall notify the Cloud Service Providerin writing of the exercise of its right to terminate the empanelment within 14 days, indicating the contractual obligation(s) in the application document for which the Cloud Service Provideris in default.

3. Conflict of Interest

a. Applicant shall furnish an affirmative statement as to the absence of, actual or potential conflict of interest on the part of the Applicant or any prospective subcontractor due to prior, current, or proposed contracts, engagements, or affiliations with MeitY. Additionally, such disclosure shall address any / all potential elements (time frame for service delivery, resource, financial or other) that would adversely impact the ability of the Applicant to complete the requirements as given in the application document. Please use form given in Annexure- 8 (Undertaking on Absence of Conflict of Interest) for making declaration to this effect.

4. Termination for Default

a. In an event where MeitY believes that the service provideris in Material Breach of its obligations under the Empanelment Terms, MeitY may, without prejudice to any other remedy for breach of terms of empanelment, terminate the Empanelment in whole or part upon giving a one month's prior written notice to the Cloud Service Provider. Any notice served pursuant to this Clause shall give reasonable details of the Material Breach, which could include the following events and the termination will become effective:

i. Service providerbecomes insolvent, bankrupt, resolution is passed for the winding up of the service provider's organization;

ii. Information provided to MeitY is found to be incorrect;

iii. Empanelment conditions are not met as per the requirements of the application document;

iv. Misleading claims about the empanelment status are made;

v. If the Cloud Service Providerfails to perform any other obligation(s) under the empanelment terms.

b. In case of such a breach, MeitY will serve thirty days written notice for curing this Breach. In case the breach continues, after the expiry of such notice period, two more reminders, each giving a time of 15 days to CSP to cure the breach, shall be served. In case the breach continues, after the expiry of the second reminder, MeitY will terminate the Empanelment. After the Empanelment is terminated, the CSP shall not be able to reapply for the Empanelment before the end of one year from the date of termination of the Empanelment.

c. In the event, MeitY terminates the Empanelment in whole or in part, the Government Department(s) (that have signed the MSA with the Cloud Service Provider) may procure, upon such terms and conditions as it deems appropriate, services similar to those undelivered, and the service providershall be liable to the Government Department(s) for any excess costs for such similar services where such excess costs shall not exceed 10% of the value of the undelivered services. However, the Cloud Service Providershall continue to work with the Government Department to the extent not terminated. On termination, the exit management and transition provisions as per the Master Services Agreement will come into effect.

5. Confidentiality

a. The Cloud Service Providerwill be exposed, by virtue of the agreed activities as per the application document, to internal business information of MeitY and other Government Departments. The service providerwould be required to provide an undertaking that they will not use or pass to anybody the data/information derived from the project in any form. The service providermust safeguard the confidentiality of MeitY's and Government Department's business information, applications and data. For this, service provideris required to sign Non-disclosure agreement with MeitY and Government Department (for the respective project).

b. Disclosure of any part of the afore mentioned information to parties not directly involved in providing the services requested, unless required to do so by the Court of Law within India or other Statutory Authorities of Indian Government, could result in premature termination of the Empanelment. The MeitY may apart from blacklisting the Cloud Service Provider, initiate legal action against the Cloud Service Providerfor breach of trust. The Cloud Service Providershall also not make any news release, public announcements or any other reference on application document or empanelment agreement without obtaining prior written consent from the MeitY.

c. Service providershall use reasonable care to protect confidential information from unauthorised disclosure and use.

6. **Arbitration**: If, due to unforeseen reasons, problems arise during the progress of the empanelment leading to disagreement between the MeitY and the service provider(or the Government Department and the service provider), both MeitY (and the Government Department as the case may be) and the Cloud Service Providershall first try to resolve the

same amicably by mutual consultation. If the parties fail to resolve the dispute by such mutual consultation within twenty-one days, then depending on the position of the case, either MeitY (or the Government Department as the case may be) or the Cloud Service Providercan give notice to the other party of its intention to commence arbitration and the applicable arbitration procedure will be as per Indian Arbitration and Conciliation Act, 1996, and the venue of the arbitration will be New Delhi (or a city as determined by the Government Department in its MSA).

7. Indemnification

a. There shall be no infringement of any patent or intellectual & industrial property rights by the Cloud Service Provideras per the applicable laws of relevant jurisdictions, having requisite competence, in respect of the Deliverables or any part thereof, supplied under the Empanelled Terms. Cloud Service Providershall indemnify MeitY (and the Government Department) against all cost/claims/legal claims/liabilities arising from third party claim at any time on account of the infringement or unauthorized use of patent or intellectual & industrial property rights of any such parties.

8. Governing law and Jurisdiction: This Empanelment Award and any dispute arising from it, whether contractual or non-contractual, will be governed by laws of India and subject to arbitration clause, subject to the exclusive jurisdiction of the competent courts of New Delhi, India.

The Applicants shall abide by the terms of the Consolidated FDI policy 2017 and all its revisions/ amendments, addendums from time to time. In case any Applicant is found in violation of the terms of the FDI policy during the process of empanelment or during the empanelment period, they shall be immediately de-empanelled and barred from any future empanelment.

9. Limitation of Liability

a. The liability of service provider(whether in contract, tort, negligence, strict liability in tort, by statute or otherwise) for any claim in any manner related to the Agreement, including the work, deliverables or services covered by the Agreement, shall be the payment of direct damages only which shall in no event in the aggregate exceed the total contract value (contract with the Government Department). The liability cap given under this Clause shall not be applicable to the indemnification obligations.

b. In no event shall either party be liable for any consequential, incidental, indirect, special or punitive damage, loss or expenses (including but not limited to business interruption, lost business, lost profits, or lost savings) even if it has been advised of their possible existence.

c. The allocations of liability in this clause represent the agreed and bargained-for understanding of the parties and compensation for the Services reflects such allocations. Each Party has a duty to mitigate the damages and any amounts payable under an indemnity that would otherwise be recoverable from the other Party pursuant to the Empanelment

Award by taking appropriate and commercially reasonable actions to reduce or limit the amount of such damages or amounts.

10. Relationship

a. Nothing mentioned herein shall be construed as relationship of master and servant or of principal and agent as between "MeitY" (or the Government Department) and the "Applicant". No partnership shall be constituted between MeitY (or the Government Department) and the Applicant by virtue of this empanelment nor shall either party have powers to make, vary or release their obligations on behalf of the other party or represent that by virtue of this or any other empanelment a partnership has been constituted, or that it has any such power. The Applicants shall be fully responsible for the services performed by them or on their behalf.

b. Neither party shall use the other parties name or any service or proprietary name, mark or logo of the other party for promotional purpose without first having obtained the other party's prior written approval.

11. De-Empanelment of Cloud Service offerings

a. The Cloud Service Offerings of the CSP shall be de-empanelled, under the following circumstances

   i. If the CSP does not register on GeM platform within 04 weeks of issue of Award of empanelment letter.

   ii. If the CSP registers on GeM platform but doesn't list its empanelled Cloud Services on GeM platform in a period of 04 weeks from the issue of Award of empanelment letter.

   iii. If a CSP is blacklisted by any User Department under any circumstances.

   iv. If MeitY receives a complaint against a CSP from a User Department and finds it in violation of the empanelment guidelines

b. If a CSP wishes to get one of its empanelled Cloud Service de-empanelled, the CSP shall give a 90 days advance notice in writing to MeitY and all the User Departments where the CSP is offering the said service, specifying the reason for applying for the de-empanelment. However, the CSP shall be bound to perform its obligation under the contract that it had entered with the User Department prior to submitting this notice.

12. Fraud and Corruption

a. MeitY requires that the Applicants engaged through this process must observe the highest standards of ethics during the performance and execution of the awarded project(s). The following terms apply in this context:

b. MeitY will reject the application for empanelment if the Applicant recommended for empanelment, has been determined by MeitY to having been engaged in corrupt, fraudulent, unfair trade practices, coercive or collusive.

c. These terms are defined as follows:

   i. "Corrupt practice" means offering, giving, receiving or soliciting of anything of value to influence the action of MeitY or any Government Department during the tenure of empanelment.

   ii. "Fraudulent practice" means a misrepresentation of facts, in order to influence a procurement process or the execution of a contract, to MeitY, and includes collusive practice among Applicants (prior to or after Proposal submission) designed to establish proposal prices at artificially high or non-competitive levels and to deprive MeitY of the benefits of free and open competition.

   iii. "Unfair trade practices" means supply of services different from what is ordered on or change in the Scope of Work which was agreed to.

   iv. "Coercive practices" means harming or threatening to harm, directly or indirectly, persons or their property to influence their participation during the period of empanelment.

   v. "Collusive practices" means a scheme or arrangement between two or more Applicants with or without the knowledge of the MeitY, designed to establish prices at artificial, non-competitive levels;

d. MeitY will reject an application for award if it determines that the Applicant recommended for award has, directly or through an agent, engaged in corrupt, fraudulent, unfair trade, coercive or collusive practices in competing for any assigned project during the empanelment.

11. Annexure – 1 - Application Response Cover Letter

Original signed copy on company letterhead

[Date]

To,

Mr. KshitijKushagra
Scientist E/Addl. Director
Ministry of Electronics and Information Technology
Electronics Niketan, 6, CGO Complex
New Delhi-110 003
Tel: +91-11- 24301373

Dear Sir,

Ref: Response to Application for Empanelment of Cloud Service Offerings of Cloud Service Providers (CSP)

Having examined the Application, we, the undersigned, submit our response as below:

1 We agree to abide by this Application, consisting of this letter, with all the annexures, duly signed, valid for a period of 180 days from the submission date specified in this application document.

2 We hereby declare that all the information and statements in this proposal are true and accept that any misinterpretation contained in it may lead to our disqualification.

3 We understand you are not bound to accept any proposal that you may receive.

The following persons will be the empaneled representative of our company/ organization for all future correspondence between the MeitY and our organization.

Organization	Name: Address: Phone:
Primary Contact	Name: Title: Phone: Email:
Secondary Contact	Name: Title: Phone: Email:
Executive Contact	Name: Title: Phone: Email:

We fully understand that in the event of any change in our contact details, it is our responsibility to inform MeitY about the new details. We fully understand that MeitY shall not be responsible for non-receipt or non-delivery of any communication and/or any missing communication from MeitY to us, in the event that reasonable prior notice of any change in the authorized person(s) of the company is not provided to MeitY.

We confirm that the information contained in this response or any part thereof, including its exhibits, and other documents and instruments delivered or to be delivered to MeitY is true, accurate, verifiable and complete. This response includes all information necessary to ensure that the statements therein do not in whole or in part mislead MeitY in its short-listing process.

We fully understand and agree to comply that on verification, if any of the information provided here is found to be misleading, we are liable to be dismissed from the selection process or, in the event of our selection, our registration is liable to be terminated.

We agree for unconditional acceptance of all the terms and conditions set out in this application document. We hereby declare that in case our Cloud services get empaneled, we shall

acknowledge and accept the Letter of Award of registration as per the requirements of the application document within 30 working days from the date of notice of award.

We agree that you are not bound to accept any response that you may receive from us. We also agree that you reserve the right in absolute sense to reject all or any of the products/ services specified in this application / proposal.

It is hereby confirmed that I/We are entitled to act on behalf of our company /corporation/firm/organization and empowered to sign this document as well as such other documents, which may be required in this connection.

Dated this _____Day of _____**2020**

(Signature) (In the capacity of)

(Name)

Duly empaneled to sign the Tender Response for and on behalf of:

(Name and Address of Company) Seal/Stamp of Applicant

Witness Signature:

Witness Name:

Witness Address:

(Company Seal)

CERTIFICATE AS TO AUTHORISED SIGNATORIES

I,....., the Company Secretary of ....., certify that ..... who signed the above Application is empaneled to do so and bind the company by authority of its board/ governing body.

Date:

Signature:

(Company Seal)

(Name)

List of Enclosures:

1. A certified true copy of the corporate sanctions / approvals authorizing its empaneled representative to sign/act/execute documents forming part of this proposal including various application documents and binding contract
2. Envelop super-scribed "Pre-qualification Response" as per the format provided in Annexure - 6
3. Envelop super-scribed "Technical Response" as per the format provided in Annexure - 7.

12. Annexure – 2 - Acceptance to offer Basic Cloud Services as defined in Cloud Services Bouquet of MeitY

(Original signed copy on the company letterhead)

[Date]

To,

Mr. KshitijKushagra
Scientist E/Addl. Director
Ministry of Electronics and Information Technology
Electronics Niketan, 6, CGO Complex
New Delhi-110 003
Tel: +91-11-24301373

Sub: Acceptance to offer Basic Cloud Services as defined in Cloud Services Bouquet of MeitY

Ref: Your Office Letter No. _____ dated_____

Dear Sir,

This is in reference to the subject cited above. We hereby convey our acceptance to offer all the "Basic Cloud Services" as defined in the Cloud Services Bouquet, under at least one of the Cloud Deployment Models (Public Cloud, Virtual Private Cloud and Government Community Cloud).

It is hereby confirmed that I/We are entitled to act on behalf of our company /corporation/firm/organization and empowered to sign this document as well as such other documents, which may be required in this connection.

Dated this (date / month / year)

Authorized Signature [in full and initials]:

Name of the Authorized Signatory:

Designation of the Authorized Signatory:

Seal / Stamp of the Company:

13. Annexure – 3 - Basic Cloud Services Empanelment Form

***Note**: Response to all the fields below are mandatory and to be submitted by the Cloud Service Provider*

Basic Cloud Services as specified in the Cloud Services Bouquet*								
Sr. No	**Service Name**	**Service Description (max 200 words)**	**Deployment Model**	**Service Model**	**Charging / Pricing Model#**			**Data Center facility name and address from where service is proposed to be offered**
			Public Cloud / Virtual Private Cloud / Government Community Cloud	**IaaS/PaaS /SaaS**	**Hourly (Yes/No)**	**Monthly (Yes/No)**	**Yearly (Yes/No)**	
1	Virtual Machine Package	<Description>	Public Cloud	IaaS	Yes	Yes	Yes	
2	.							
3	.							
4	.							
5	.							
6	.							
	Add as many rows as required							

* All "Basic Cloud Services" as defined in the Cloud Services Bouquet (Refer Annexure 15) are mandatory. No deviation from the Cloud Services Bouquet is allowed. CSPs are also required to submit their acceptance to offer all "Basic Cloud Services" as defined in Cloud Services Bouquet, under at least one of the Cloud Deployment Models (Public Cloud, Virtual Private Cloud and Government Community Cloud) as per Annexure 2.

Please refer to "Cloud Services Bouquet" prepared by MeitY. No deviation is allowed on the "Charging / Pricing Model" of the Cloud services.

14. Annexure – 4 - Advanced Cloud Services Empanelment Form

***Note**: Advance Cloud Services are **OPTIONAL** for CSPs. Please refer Cloud Services Bouquet for more information.*

Advanced Cloud Services as specified in the Cloud Services Bouquet								
Sr. No	**Service Name**	**Service Description (max 200 words)**	**Deployment Model**	**Service Model**	**Charging / Pricing Model**			**Data Centre facility name and address from service is proposed to be offered**
			Public Cloud / Virtual Private Cloud / Government Community Cloud	**IaaS/PaaS /SaaS**	**Hourly (Yes/No)**	**Monthly (Yes/No)**	**Yearly (Yes/No)**	
1	PostgreSQL	<Description>	Public Cloud	PaaS	No	Yes	Yes	
2	.							
3	.							
4	.							
5	.							
6	.							
7	.							
	Add as many rows as required							

15. Annexure – 5 - Pre-Qualification Criteria

The Responses received shall be evaluated based on the following criteria as specified below.

i. The Applicant, as a single legal entity, must be incorporated and registered in India under the Indian Companies Act 1956 or a Limited Liability Partnership (LLP) registered under the LLP Act, 2008 or Indian Partnership Act 1932 and should have been in operation in India for minimum of three years

ii. The Applicant, as a single legal entity or its holding company, must have a positive Net Worth in each of the last two financial years **(2017-18 and 2018-19**).

iii. The Applicant, as a single legal entity or its holding company, must have a cumulative revenue of minimum INR 20 Crores from the Data Centre related services during the last two financial years **(2017-18 and 2018-19**) either in India or Globally.

iv. The Applicant, as a single legal entity or its holding company, should be currently delivering Infrastructure as a Service offering in India or globally (IaaS as defined in this document providing on-demand Storage and VMs). The IaaS offering shall provide for tools or capabilities that enable users to unilaterally provision / order, manage, and use the Cloud services:

    a) Service Management & Provisioning (Service Provisioning and De-Provisioning near real-time of provisioning request, SLA Management, and Utilization Monitoring)

    b) Provide visibility into service via dashboard

    c) User / Admin Portal (User Profile Management, Trouble Management)

    d) Enterprise grade SLAs with an assured uptime of 99.5% (measured as Total Uptime Hours / Total Hours within the Month), SLA measured at the VM Level and SLA measured at the Storage level

    e) Cloud services should be accessible via internet and MPLS

v. The Data Center Facility (or each of the facilities as the case may be[1]) proposed for empanelment (facility from where the Cloud Service Offerings are proposed to be offered) must meet the following criteria:

    a) The Data Center Facility must be within India, should be currently operational and have a minimum capacity of 50 Racks being operational

    b) The Data Center Facility shall at a minimum have:

        i. Routers, Firewalls, LAN, WAN, Internet Access, and Hosting Centers, Backup, Operations Management, and Data Management

        ii. Security & Data Privacy (Data & Network Security including Anti-Virus, Virtual Firewall, Multi Factor Authentication, VPN, IPS, Log Analyzer / Syslog, SSL, DDOS Protection, HIDS / NIDS, Rights Management, SIEM,

Integrated Vulnerability Assessment, SOC, Private Virtual Zones, Data Privacy, Data Encryption, Certifications & Compliance, Authentication & Authorization, and Auditing & Accounting)

iii. Conform to at least Tier III standard, preferably certified under TIA 942 or Uptime Institute certifications by a 3rd party

iv. Assured protection with security built at multiple levels

v. Certified for ISO 27001:2013

vi. NOC offered for the Data Center and the managed services quality should be certified for ISO 20000-1:2018

vi. The Applicant, as a single legal entity or its holding company, should not be blacklisted for its Data Center / Cloud Services by Central Government Ministry or Department of Government of India. Applicant, as a single legal entity or its holding company, also should not be under any legal action for indulging in corrupt practice, fraudulent practice, coercive practice, undesirable practice or restrictive practice with any Central Government Ministry or Department of Government of India. The Applicant shall submit a self-declaration on the company letter head, signed by authorized signatory.

IN CASE THE APPLICANT CHOOSES TO OFFER THE CLOUD SERVICES PROPOSED FOR EMPANELMENT FROM MULTIPLE DATA CENTER FACILITIES, EACH OF THE DATA CENTER FACILITIES SHALL MEET THE CRITERIA

16. Annexure – 6 - Form for Submission of Pre-qualification Information

The pre-qualification information should address all the pre-qualification criteria as specified in the Annexure - 5 and should contain details of how the Applicant satisfies the pre-qualification criteria.

1. **General Details of the Organization**
   - **a.** This part must include a general background of the respondent organization **(limited to 400 words**) providing the details of the relevant services offered by the Organization
2. **Incorporation Details of the Organization**
   - a. Incorporation details of the organization as per the format provided below. Enclose the mandatory supporting documents listed in format.

Details of the Organization	
Name of organization	
Nature of the legal status in India	
Legal status reference details	
Nature of business in India	
Date of Incorporation	
Date of Commencement of Business	
Address of the Headquarters	<<street and mailing addresses, phone, fax and email>>
Address of the Registered Office in India	<<street and mailing addresses, phone, fax and email>>
Address of the Data Center Facility	<<street and mailing addresses, phone, fax and email>>
Other Relevant Information	
Mandatory Supporting Documents: a) Certificate of Incorporation from Registrar of Companies(ROC)	

3. **Incorporation Details of the Holding Company (Only required if some of the pre-qualification conditions are being met by the Applicant's Holding Company)**

a. Incorporation details of the holding company as per the format provided below.

Details of the Organization	
Name of organization	
Nature of the legal status in India	
Legal status reference details	
Nature of business	
Date of Incorporation	
Date of Commencement of Business	
Address of the Headquarters	<<street and mailing addresses, phone, fax and email>>
Address of the Registered Office in India, if any	<<street and mailing addresses, phone, fax and email>>
Nature of Relationship with the Applicant's Organization (Holding Company – Subsidiary Company Relationship)	
Address of the Data Center Facility	<<street and mailing addresses, phone, fax and email>>
Other Relevant Information	

4. **Financial Details of the Organization**

a. Financial details of the organization as per the format below. Enclose the mandatory supporting documents listed in format.

Financial Information of <<*Applicant / Holding Company*>>		
	FY 2017-18	**FY 2018-19**
Net Worth (in INR Crores)		
Revenue from the Data Centre related services (in INR Crores)		
Other Relevant Information		
Mandatory Supporting Documents: a. Auditor Certificate for the last two financial years: 2017-18 and 2018-19 indicating the Net Worth and Revenue from the Data Centre related services		

5. Details of the IaaS Cloud Service Offerings either in India or Globally

Details of the IaaS Cloud Service Offerings of <<*Organization / Holding Company*>>	
IaaS services are offered by	Applicant as a Single Legal Entity OR Holding Company of the Applicant
Countries where the IaaS services are offered	
Start date of offering of the Infrastructure as a Service offerings as defined in this document providing on-demand Storage and VMs from the Data Center Facility	Month & Year
Conformance with respect to: The IaaS offering shall provide for tools or capabilities that enable users to unilaterally provision / order, manage, and use the Cloud services	<<Yes / No>>
The portal along with the service catalogue of the Applicant's current IaaS offerings.	
Other Relevant Information	

6. Details of the Data Center Facility and Cloud Service Offerings in India

(IN CASE THE APPLICANT CHOOSES TO OFFER THE CLOUD SERVICES PROPOSED FOR EMPANELMENT FROM MULTIPLE DATA CENTER FACILITIES, PLEASE PROVIDE THE DETAILS OF EACH OF THE DATA CENTER FACILITIES IN THE FORMAT BELOW)

Details of the Data Center Facility	
Address of the Data Center Facility	<<street and mailing addresses, phone, fax and email>>
Month / Year of Starting the Data Center Operations	Month & Year
Operational Capacity (Number of Racks)	<<Number >>
Availability of Routers, Firewalls, LAN, WAN, Internet Access, and Hosting Centers, Backup, Operations Management, and Data Management	<<Yes / No>>
Security Features available including Physical Security (Security & Data Privacy (Data & Network Security including Anti-Virus, Virtual Firewall, Multi Factor Authentication, VPN, IPS, Log Analyzer / Syslog, SSL, DDOS Protection, HIDS / NIDS, Rights Management,	<<Yes / No>>

Details of the Data Center Facility	
SIEM, Integrated Vulnerability Assessment, SOC, Private Virtual Zones, Data Privacy, Data Encryption, Certifications & Compliance, Authentication & Authorization, and Auditing & Accounting))	
Tier Level and certifications (Conformance to at least Tier III standard, preferably certified under TIA 942 or Uptime Institute certifications by a 3rd party)	<<Yes / No>> In case certified, details of the Certification
Certified for ISO 27001:2013	<<Yes / No>> Details of the Certification
NOC offered for the Data Center and the managed services quality should be certified for ISO 20000-1:2018	<<Yes / No>> Details of the Certification
Other Relevant Information	
Mandatory Supporting Documents: a) ISO 27001 (year 2013) Certification b) ISO 20000-1:2018 Certification Details c) TIA 942 or UPTIME Certification d) ISO 27017 (2015) Certification e) ISO 27018 (2019) Certification	

7. **Self-declaration on Blacklisting from the Applicant On company letter head, signed by authorized signatory**

   a. The Applicant, as a single legal entity or its holding company (if applicable), should not be blacklisted for its Data Center Operations by Central Government Ministry or Department of Government of India. Applicant, as a single legal entity or its holding company (if applicable), also should not be under any legal action for indulging in corrupt practice, fraudulent practice, coercive practice, undesirable practice or restrictive practice with any Central Government Ministry or Department of Government of India. The Applicant shall submit a self-declaration on the company letter head, signed by authorized signatory.

17. Annexure – 7 - Form for Submission of Technical Compliance

The technical proposal should address all the areas / sections as specified in the application document and should contain a detailed description of how the Applicant will provide the required services outlined in this application document. It should articulate in detail, as to how the Applicant's Technical Solution meets the requirements specified in the application document. The technical proposal must not contain any pricing information.

The technical proposal shall contain the following:

1. **Acceptance to Offer Basic Cloud Services** as defined in Cloud Services Bouquet of MeitY, under Annexure - 2

2. **Details of Cloud Services proposed to be empaneled as per the Bouquet of Cloud Services prepared by MeitY, under** Annexure – 3 **and** Annexure - 4 (available at https://meity.gov.in/writereaddata/files/cloud_services_bouquet.pdf)

3. **Undertaking on Absence of Conflict of Interest** as per the format provided under Annexure-8

4. **Undertaking on Legal Compliance** as per the format provided under Annexure - 9

5. **Requirements Compliance Matrix against each of the Cloud Service Offerings proposed to be Empaneled** as per the format provided under Annexure-10

18. Annexure – 8 - Undertaking on Absence of Conflict of Interest

Original signed copy on company letterhead

[Date]

To,

Mr. KshitijKushagra
Scientist E/Addl. Director
Ministry of Electronics and Information Technology
Electronics Niketan, 6, CGO Complex
New Delhi-110 003
Tel: +91-11-24301373

Dear Sir,

Ref: Undertaking on Absence of Conflict of Interest

I/We as Applicant do hereby undertake that there is absence of, actual or potential conflict of interest on the part of our organization or any prospective subcontractor due to prior, current, or proposed contracts, engagements, or affiliations with MeitY. I/We also confirm that there are no potential elements (time frame for service delivery, resource, financial or other) that would adversely impact the ability of our organization to comply with the requirements as given in the application document.

We undertake and agree to indemnify and hold MeitY harmless against all claims, losses, damages, costs, expenses, proceeding fees of legal advisors (on a reimbursement basis) and fees of other professionals incurred (in the case of legal fees & fees of professionals, reasonably) by MeitY and/or its representatives, if any such conflict arises later.

Yours faithfully,

Authorised Signatory

Designation

19. Annexure – 9 - Undertaking on Legal Compliance

Original signed copy on company letterhead

[Date]

To,

Mr. KshitijKushagra
Scientist E/Addl. Director
Ministry of Electronics and Information Technology
Electronics Niketan, 6, CGO Complex
New Delhi-110 003
Tel: +91-11-24301373

Dear Sir,

Ref: Undertaking on Legal Compliance

I/We as Applicant do hereby comply to the IT Act 2000 (including 43A) and amendments thereof; meet ever evolving Security Guidelines specified by CERT-In, and meet any security requirements published (or to be published) by MeitY or any standards body setup / recognized by Government of India from time to time and notified to the CSP by MeitY as a mandatory standard.

We confirm that all the services acquired under this application document including data will be guaranteed to reside in India and there shall not be any legal frameworks outside Indian Law that will be applicable to the operation of the service (and therefore the information contained within it).

Yours faithfully,

Authorised Signatory

Designation

20. Annexure – 10 - Format for Requirement Compliance Matrix

Sr. No.	Requirements as specified in the Application	Comply (Y for Yes / N for No)	Details on how the offerings of the Cloud Service Providers meets the requirement
1.	**Section 6.1.1.A** 'Requirements specific to Public Cloud'		
2.	**Section 6.1.1.B** 'Requirements specific to Virtual Private Cloud'		
3.	**Section 6.1.1.C** 'Requirements specific to Government Community Cloud'		
4.	**Section 6.1.2** 'General Requirements for all Cloud Deployment Model'		
5.	**Section 6.2.1** Specific Requirements for 'Infrastructure as a Service (IaaS)'		
6.	**Section 6.2.2** 'Specific Requirements for Platform as a Service (PaaS)'		
7.	**Section 6.2.3** 'Specific Requirements for Software as a Service (SaaS)'		
8.	**Section 6.2.4** 'General requirements for all Cloud Service Models'		
9.	Section 7 **Compliance Requirements**		

Note:

i. Compliance: The Applicants must comply with the mandatory requirements as mentioned in the Annexure above, on the date of submission of the Application. If the Applicant complies with the mandatory requirements, the Applicant should enter a "Y" or "Yes" in the column.

21. Annexure – 11 - Undertaking on Data Center Service Arrangements

*[Note: The below undertaking needs to be obtained in original from **each** of the Data Center Providers whose facilities are proposed to be leveraged for offering the Cloud services. The undertaking needs to be signed & stamped by Signatory of the Data Center Provider. The same needs to be countersigned & stamped by the Signatory of the CSP (Applicant) as well.]*

[Date]

To,

KshitijKushagra
Scientist E/ Addl. Director
Department of Electronics and Information Technology
Electronics Niketan, 6 CGO Complex
New Delhi-110003

Dear Sir,

Ref: Undertaking on Data Center Services Arrangements

This is with reference to the Application for Empanelment of Cloud Services offered by Cloud Service Providers, released by Ministry of Electronics and Information Technology (MeitY).

This is to certify that I/We/ am/are the Cloud Service Providers (CSP) and I/We confirm that we have an agreement and due authorization with Data Center Service Provider to utilize their infrastructure for providing the Cloud services proposed by the CSP/Applicant to be empaneled by MeitY.

S. No.	Data Center proposed to be used for offering Cloud Services to Government Departments (Data Center name with complete address)	Please specify, if it is your (CSP's) own Data Centre / 3rd Party Data Centre	Total No. of racks exclusive and dedicated to you (CSP) in the Data Center facility, proposed to be empaneled	Please specify lease agreement validity date in DD-MMM-YYYY format {between you (CSP) and 3rd party Data Center facility provider}
1				

Yours faithfully,

Signatory
(Cloud Service Provider)
Designation & Seal of organization
[Date]

Signatory
(Data Center Service Provider)
Designation & Seal of organization
[Date]

22. Annexure – 12 - Request for Clarification Format

Applicant's Request for Clarification on Application Document			
Name of the Applicant submitting the request		Name and position of person submitting request	Full formal address of the Applicant including phone, fax and email points of contact
S. No	Application document reference(s) (section number/ page)	Content of Application document requiring clarification	Points on which clarification required
1.			
2.			

23. Annexure – 13 - Compliance and Certification Requirements

The Cloud Service Provider is required to provide the following certification details printed and duly signed on CSPs Letter head and submit a copy of each certificate mentioned in the table.

[Date]

To,

KshitijKushagra
Scientist E/ Addl. Director
Department of Electronics and Information Technology
Electronics Niketan, 6 CGO Complex
New Delhi-110003

Dear Sir,

Ref: Compliance and Certification Requirements

This is with reference to the Application for Empanelment of Cloud Services offered by Cloud Service Providers, published by Ministry of Electronics and Information Technology (MeitY).

This is to certify that I/We/ am/are the Cloud Service Providers (CSP) and I/We confirm that we comply with below certifications as specified.

Certification	Certificate Number	Issued To	Issued By	Issue Date	Expiration Date
ISO 27001:2013					
ISO 20000-1:2018					
ISO 27017:2015					
ISO 27018:2019					
TIA-942 / UPTIME (Tier III or higher)					

Yours faithfully,

Authorized Signatory
Designation

24. Annexure – 14 - Format for Earnest Money Deposit (EMD)

[Date]
From:
Bank _____

To,

Pay and Accounts Officer
Ministry of Electronics and Information Technology
Electronics Niketan , 6, CGO Complex
New Delhi-110 003

1. In consideration of _____ (hereinafter called the "MeitY") represented by _____, on the first part and M/s _____ of _____ (hereinafter referred to as "Applicant") on the Second part, having agreed to accept the Earnest Money Deposit of Rs. _____ (Rupees_____) in the form of Bank Guarantee for the Application for Empanelment of Cloud Service Offerings of Cloud Service Providers (CSPs), we _____ (Name of the Bank), (hereinafter referred to as the "Bank"), do hereby undertake to pay to the MeitY forthwith on demand without any demur and without seeking any reasons whatsoever, an amount not exceeding _____ (Rupees _____) and the guarantee will remain valid up to a period of 225 days from the date of submission of application. It will, however, be open to the MeitY to return the Guarantee earlier than this period to the Applicant, in case the applicant has been notified by the MeitY as being unsuccessful.

2. In the event of the successful application, if the applicant fails to acknowledge and accept the Letter of Award of Empanelment from MeitY in accordance with the terms and conditions of the Empanelment Application, the EMD deposited by the applicant stands forfeited to the Government. We also undertake not to revoke this guarantee during this period except with the previous consent of the Government in writing and we further agree that our liability under the EMD shall not be discharged by any variation in the term of the said tender and we shall be deemed to have agreed to any such variation.

3. No interest shall be payable by the MeitY to the Applicant on the guarantee for the period of its currency.

4. Notwithstanding anything contained hereinabove:

a) Our liability under this Bank Guarantee shall not exceed and is restricted to Rs._____(Rupees_____only)

b) This Guarantee shall remain in force up to and including _____ .

c) Unless the demand/claim under this guarantee is served upon us in writing before _____ all the rights of MeitY under this guarantee shall stand automatically forfeited and we shall be relieved and discharged from all liabilities mentioned hereinabove.

Dated this_____day of _____ 2020

For the Bank of _____
(Agent/Manager)

25. Annexure – 15 - Cloud Services Bouquet

The Cloud services, listed under this section, have been categorized into “Basic Cloud Services” and “Advanced Cloud Services”. The Cloud services listed under the “Basic Cloud Services” are mandatory for all CSPs to offer to the Government Organizations under at least one of the empaneled Cloud Deployment Models. However, the Cloud services listed under the “Advanced Cloud Services” category are optional for the CSPs to offer.

Cloud services, under both the categories, are to be listed on the Government eMarketplace(GeM) platform once they have been successfully empanelledby the MeitY.If a CSP wants to list Cloud services, which are not covered under this document, it needs to follow the due process specified by MeitY to get its services first empanelled with MeitY under the “Advanced Cloud Services”.

While listing their Cloud services on the GeM platform, CSPs will be required to classify their Cloud services into one of the three service models – Infrastructure as a Service (IaaS), Platform as a Service (PaaS) and Software as a Service (SaaS) – based on the controls identified and defined by MeitY in its Cloud Services EmpanelmentRFP. CSPs shall also be provided with the option of specifying their Cloud service capabilities on the GeM platform while showing the service definition and service procurement parameters as identified and defined for those services in this document.

For majority of the Cloud services listed in this document, per unit price for various ranges of quantities will be discovered to ensure that Government Organizations get better prices as the quantity increases, e.g., for “Active Directory Services”, monthly and yearly price per user will be discovered for the users up to 100, between 101 and 200, between 201 and 300, between 301 and 400, between 401 and 500, and more than 500.

All the Cloud services mentioned in this bouquet are mandatorily required to meet all the controls, including technical, security and legal, specified in the Cloud Services Empanelment RFP issued by MeitY.

To keep this section clutter free, the Service Procurement Parameters for Cloud services have been provided in the drop down boxes. To see the actual values of the Service Procurement Parameters, please click on the text named “Choose an item.”

25.1 Basic Cloud Services

These services, as mentioned earlier, are mandatory for CSPs to offer. However, CSPs are not required to offer all the SKUs (combinations) of the Cloud services listed under "Basic Cloud Services" category. CSPs will be required to display prices of these basic Cloud services on the Government eMarketplace (GeM).

25.1.1 ComputeServices

This service can be used by the Government Organizations to access the virtualized servers offered by the Cloud Service Providers. This bouquet currently includes only two types of compute services – Virtual Machines and Containers. Virtual Machines have been kept under the "Basic Cloud Services" while containers have been categorized under the "Advanced Cloud Services".

1) Virtual Machine

Virtual Machines (VM) provide the basic IT Infrastructure that can be used by the Government Organizations to run their variety of workloads such as compute-intensive workload, memory-intensive workload, general-purpose workload, etc. All Virtual Machine packages, listed below, are Managed Virtual Machines. CSPs are required to list their prices on GeM platform keeping this in mind. These VMs will be provided with following mandatory inclusions without any extra cost.

Sr. No.	Category	Inclusion[1, 2]
1.	Processor	• Minimum frequency of 2.0 GHz
2.	Storage type	• 50 GB of Hard Disk Drive (HDD) storage, OR • 50 GB of Solid State Drive (SSD)storage as required by the Government Organization (additional storage, if required, may be procured separately)

Sr. No.	Category	Inclusion[1, 2]

3.	Operating System	• Any supported version of the following operating systems as per the requirement specified by the Government Department[3]
		  • Microsoft Windows Server
		  • Red Hat Enterprise Linux
		  • Oracle Linux
		  • SUSE Linux Enterprise Server
		  • CentOS Operating System
		  • Ubuntu Operating System

4.	Network	• Subnet / network segment capability should be available • VM should be firewall protected • Mapping of Private IPs to Public IPs for inbound / outbound traffic
5.	Security	• Antivirus • Identity and Access Management including Single-Sign On for managing access to Cloud servicesof the CSP

Sr. No.	Category	Inclusion[1, 2]
		• Encryption of data associated with VM • System log should be available • Multi-factor authentication • Hardening & patch management of underlying infrastructure by CSP
6.	Backup	• Entire VM data backup must be available • Backup must be taken at least every week • Backup of VM must be retained for at least 30 days.
7.	Auto scaling	• Ability to auto scale at least horizontally without bringing the virtual machine down
8.	Service Level Agreement	• Virtual Machine Uptime SLA of at least 99.5%
9.	Scheduling	• Scheduling features such as auto start, auto shut-down, etc., without requiring manual intervention
10.	Turnaround Time	• Resource (vCPU, storage, etc.) scaling up and down should be completed

Sr. No.	Category	Inclusion[1, 2]
		within 30 minutes. Alert may be provided.
11.	Virtual Machine Administration	• Basic monitoring tool and dashboard including admin access

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

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

[3] Price of VM will vary based on the operating system selected by the Government Organization.

Sr. No.	Service Name[4,5]	Service Procurement Parameter					
		Operating System	vCPU	RAM (GB)	Storage (GB)	CPU Launch Year	Physical Core to vCPU Ratio[6]
1	Virtual Machine Package[4]	Choose an item.	Choose an item.	Choose an item.	Choose an item.	Choose an item.	Choose an item.

[4] For the above configuration of Virtual Machines, hourly, monthly and yearly prices will be discovered.

[5] In addition to the already specified SKUs, CSPs are allowed to list their own SKUs of the virtual machines on the GeM platform, provided that these SKUs meet all the specified criteria including minimum inclusions.

[6]**Physical Core to vCPU ratio**

Keeping all other parameters same, it is recommended to consider following guidelines while selecting a Virtual Machine for a running a workload.

Physical Core to vCPU ratio	Recommendation
1:1	No performance issues. Recommended for business critical workloads.
1:2	Optimum performance. Recommended for compute intensive workloads.
1:3	Little performance degradation may be experienced depending on the workload. Recommended for regular and low-priority production workloads.
1:4	May cause performance scarcity. Recommended for non-production and test/development environment.

25.1.2 Storage Services

1) Block Storage

Used to store data in volumes as blocks. Because the volumes are treated as individual hard disks, block storage works well for storing a variety of applications.

Sr. No.	Service Name[1]	Service Procurement Parameter		
		Storage Type	Storage Amount (GB)	IOPS
1	Block Storage as a Service	Choose an item.	Choose an item.	Choose an item.

[1] Hourly, monthly and yearly price of the above configuration of storage will be discovered.

2) Object Storage

Used to store unstructured data such as photos, audio, videos, etc., as objects.

Sr. No.	Service Name[1]	Service Procurement Parameter
		Storage Amount (GB)
1	Object Storage as a Service	Choose an item.

[1] Hourly, monthly and yearly price of the above configuration of storage will be discovered.

3) File Storage

Provides a centralized, hierarchical, and highly accessible location for files, and generally comes at a lower cost than block storage.

Sr.	Service Name[1]	Service Procurement Parameter

No.		Storage Amount (GB)
1	File Storage as a Service	Choose an item.

[1] Hourly, monthly and yearly price of the above configuration of storage will be discovered.

4) Archival Storage

Used to store information which is accessed infrequently.

Sr. No.	Service Name[1]	Service Procurement Parameter
		Storage Amount (GB)
1	Archival Storage as a Service	Choose an item.

[1] Hourly, monthly and yearly price of the above configuration of storage will be discovered.

25.1.3 Database Services

1) ManagedDatabase as a Service

Database as a Service is a managed service offering by the Cloud Service Providers wherein in operating system and all low level components such as drivers, I/O, network, etc. are managed and optimized by the Cloud Service Providers. All objects created using "Database as a Service" are transparent to the underlying operating system. Activities such as OS management, antivirus, encryption, hardening, etc. are included under this service. Automated failover, backup & recovery, isolation & security, scaling, automated patching, advanced monitoring, and routine maintenance are responsibilities of the CSP. Each database as a service will be offered by the Cloud Service Providers with a minimum storage inclusion of 50 GB HDD or 50 GB SSD. CSPs shall be required to provide a transparent view of the database activities managed by them.

Sr. No.	Database Service Name[1]	Service Procurement Parameter				
		vCPU	RAM (GB)	Storage (GB)	CPU Launch Year	Physical Core to vCPU Ratio[7]
1	Microsoft SQL as a Service – Standard Edition	Choose an item.	Choose an item.	Choose an item.	Choose an item.	Choose an item.
2	Microsoft SQL as a Service – Enterprise Edition	Choose an item.	Choose an item.	Choose an item.	Choose an item.	Choose an item.
3	Microsoft SQL as a	Choose an item.	Choose an item.	Choose an item.	Choose an item.	Choose an item.

Sr. No.	Database Service Name[1]	Service Procurement Parameter				
	Service – Web Edition					

[1] For the above configuration of database as a service, hourly, monthly and yearly prices shall be discovered.

For additional managed databases services, please refer "Advanced Cloud Services" section of this document.

25.1.4 Network Services

1) Virtual Network

Sr. No.	Service Name	Service Definition	Service Procurement Parameter
1	Virtual Network	This service may be used to logically segregate the computing resources, such as virtual machines, databases, etc., within a CSP's cloud environment.	None. All CSPs provide virtual network / subnet capability by default to their customers without any extra cost. However, resources used within the virtual network / subnet may be charged by the CSPs.

2) Load Balancer

Sr. No.	Service Name	Service Definition	Service Procurement Parameter[1]
			Throughput (MBPS)

Sr. No.	Service Name	Service Definition	Service Procurement Parameter[1]
			Throughput (MBPS)
1	Application Load Balancer (Virtual/Physical)	This service may be used to distribute the traffic across many computing resources within the same site to increase the responsiveness and availability of applications.	Choose an item.
2	Network Load Balancer (Virtual/Physical)	This service may be used to balance the traffic across two WAN links (two different sites).	Choose an item.

[1]Hourly, monthly and yearly prices will be discovered for these configurations of application and network load balancers.

3) VPN Gateway

Sr. No.	Service Name	Service Definition	Service Procurement Parameter[1]	
			Bandwidth (Mbps)	No. of Site to Site Connections Required

Sr. No.	Service Name	Service Definition	Service Procurement Parameter[1]	
			Bandwidth (Mbps)	No. of Site to Site Connections Required
1	VPN Gateway – Site to Site Connection	This service may be used to establish secure site to site connectivity between the subnets in CSP's environment and Government Organization's on-premises IT infrastructure. It can also be used to provide site to site connectivity two different subnets within the CSP's Cloud environment.	Choose an item.	Choose an item.

[1] For the bandwidth mentioned above, price per site to site connection for each of the two ranges specified will be discovered.

Sr. No.	Service Name	Service Definition	Service Procurement Parameter[1]	
			Bandwidth (Mbps)	**No. of Point to Site Connections Required**
2	VPN Gateway – Point to Site Connection	This service may be used to establish a secure point to site connection between an individual client computer and a subnet in CSP's environment.	Choose an item.	Choose an item.

[1] For the bandwidth mentioned above, price per point to site connection for each of the two ranges specified will be discovered.

4) Firewall

Sr. No.	Service Name	Service Definition	Service Procurement Parameter[1]
			Throughput (MBPS)
1	Firewall (Virtual/Physical)	This service is used to monitor and control the incoming and outgoing traffic of a subnet by configuring some rules.	Choose an item.

[1]Hourly, monthly and yearly prices will be discovered for the firewall for the specified throughput.

5) Public IP

Sr. No.	Service Name[4,5]	Service Definition	Service Procurement Parameter	
			Type of IP	No. of IPs Needed
6	Public IP	This service can be used to assign Public IP(s) to resources within a subnet in the Cloud environment.	Choose an item.	Choose an item.

[4] Hourly, monthly and yearly price per Public IP will be discovered.

[5] CSPs are required to provide IPv6 support without any extra cost.

6) Web Application Firewall

Sr. No.	Service Name	Service Definition	Service Procurement Parameter[1]
			Throughput (MBPS)
1	Web Application Firewall	This service may be used to create rules to protect web applications from unwanted web traffic, hacks, brute force attacks, cross-site scripting, SQL injection, and other common exploits. The WAF must also provide protection against the OWASP top ten risks.	Choose an item.

[1]Hourly, monthly and yearly prices will be discovered for the Web Application Firewall for the specified throughput.

25.1.5 Security Services

1) Identity and Access Management

Sr.	Service Name	Service Definitions	Service Procurement Parameter[1]

No.			No. of Users
1	Active Directory Services	This service may be used to authenticate and authorize users and computing resources within a network by assigning and enforcing security policies.	Choose an item.

[1] For the above range of users, monthly and yearly price per user will be discovered.

25.1.6 Support Services

Sr. No.	Service Name	Minimum Inclusions*
1	Basic Support Services	(i) 24x7 access to email, chat and phone support to notify and register the incidents (ii) 24x7 support for general guidance (iii) Response to be made available within 1 hour for any kind of service / system outage
2	Enterprise Support Services	(i) Basic Support Services (ii) Response to be made available within 15 minutes for Business Critical System outage

* Monthly price for both types of support services shall be discovered.

25.2 Advanced Cloud Services

These services, as mentioned earlier, are optional for CSPs to offer. The prices of these advanced Cloud services may be displayed by the CSPs on the GeM marketplace or the Government Organizations may discover prices of these advanced Cloud services through the bid process functionality available on the GeM platform.

25.2.1 Compute Services

1) Containers

Containers are the lightweight alternatives to Virtual Machines. Containers allow to encapsulate an application's code, libraries, configuration and other dependent files into one single package. This packaging of the application and its dependent files offers improved developer productivity and environmental neutrality. The developers can continue focusing on improving/updating their applications without being worried about the different environments, such as development, test and production, in which their applications would be deployed and run.

Sr. No.	Service Name[1]	Service Procurement Parameter	
		vCPU	RAM (GB)
1	Container as a Service	Choose an item.	Choose an item.

[1] For the above configuration of containers, per second price will be discovered keeping their intrinsic nature in consideration. Government Organizations will be charged separately for storage and other Cloud services that they consume.

25.2.2 Database Services

1) Managed Database as a Service

Database as a Service is a managed service offering by the Cloud Service Providers wherein in operating system and all low level components such as drivers, I/O, network, etc. are managed and optimized by the Cloud Service Providers. All objects created using "Database as a Service" are transparent to the underlying operating system. Activities such as OS management, antivirus, encryption, hardening, etc. are included under this service. Automated failover, backup & recovery, isolation & security, scaling, automated patching, advanced monitoring, and routine maintenance are responsibilities of the CSP. Each database as a service will be offered by the Cloud Service Providers with a minimum storage inclusion of 50 GB HDD or 50 GB SSD. CSPs shall be required to provide a transparent view of the database activities managed by them.

Sr. No.	Database Service Name[1]	Service Procurement Parameter				
		vCPU	RAM (GB)	Storage (GB)	CPU Launch Year	Physical Core to vCPU Ratio
1.	MySQL as a Service	Choose an item.	Choose an item.	Choose an item.	Choose an item.	Choose an item.
2.	PostgreSQL as a Service	Choose an item.	Choose an item.	Choose an item.	Choose an item.	Choose an item.
3.	Oracle as a Service	Choose an item.	Choose an item.	Choose an item.	Choose an item.	Choose an item.
4.	MariaDB as a Service	Choose an item.	Choose an item.	Choose an item.	Choose an item.	Choose an item.

[1] For the above configuration of database as a service, CSPs will be required to provide hourly and/or monthly and/or yearly prices on the GeM platform.

For the following list of database services, CSPs may list their services on the GeM platform clearly providing the service capabilities and service procurement parameters.

Sr. No.	Service Name[1]	Service Definition	Service Procurement Parameter
1.	NoSQL Database as a Service	This service may be used to store and retrieve data in means other than the tabular relations used in relational databases. There are many NoSQL databases available in the market, such as, MongoDB, CouchDB, Memcached, Redis, Cassandra, etc. While listing the NoSQL Database Service on GeM platform, CSPs will clearly specify the databases that they are offering and their capabilities.	To be specified by CSPs

[1] For the above configuration of database as a service, CSPs will be required to provide hourly and/or monthly and/or yearly prices on the GeM platform.

2) Database Licenses

CSPs may also offer database licenses to Government Organizations which they can use in that particular CSP's Cloud environment. These are unmanaged databases. All these databases would have enterprise support included.

Sr. No.	Service Name	Service Procurement Parameter
		No. of Licenses[1]

Sr. No.	Service Name	Service Procurement Parameter
		No. of Licenses[1]
1.	MS SQL Server 2012 Standard Edition	Choose an item.
2.	MS SQL Server 2012 Enterprise Edition	Choose an item.
3.	MS SQL Server 2014 Standard Edition	Choose an item.
4.	MS SQL Server 2014 Enterprise Edition	Choose an item.
5.	MS SQL Server 2016 Standard Edition	Choose an item.
6.	MS SQL Server 2016 Enterprise Edition	Choose an item.
7.	MS SQL Server 2017 Standard Edition	Choose an item.
8.	MS SQL Server 2017 Enterprise Edition	Choose an item.
9.	Oracle 11 Standard Edition	Choose an item.

Sr. No.	Service Name	Service Procurement Parameter
		No. of Licenses[1]
10.	Oracle 11 Enterprise Edition	Choose an item.
11.	Oracle 12 Standard Edition	Choose an item.
12.	Oracle 12 Enterprise Edition	Choose an item.
13.	MySQL Standard Edition	Choose an item.
14.	MySQL Enterprise Edition	Choose an item.
15.	PostgreSQL Enterprise Edition	Choose an item.
16.	MongoDB (NoSQL) Enterprise Edition	Choose an item.
17.	Cassandra (NoSQL) Enterprise Edition	Choose an item.
18.	IBM DB2 Version	Choose an item.

[1] For all the license ranges specified, yearly price per license will be discovered.

25.2.3 Network Services

1) Content Delivery Network

Sr. No.	Service Name	Service Definition	Service Procurement Parameter[1]
			Outbound Data Transfer (TB/Month)
1	Content Delivery Network (CDN)	CDN service may be used to securely deliver audio, video, images, data, application, etc., quickly by using the servers closest to each user. CDN reduces load time and saves bandwidth.	Choose an item.

[1] Hourly and monthly price per GB of Outbound Data Transfer will be discovered.

2) MPLS Connectivity (Port Charges)

Sr. No.	Service Name	Service Definition	Service Procurement Parameter[1]
			Throughput (MBPS)
1	MPLS Connectivity (Port Charges)	This service may be used to have a dedicated MPLS connectivity betweenGovernment Organization's	Choose an item.

Sr. No.	Service Name	Service Definition	Service Procurement Parameter[1]
			Throughput (MBPS)
		office / data centre with CSP's Cloud environment. (The User Department shall be required to pay separately to the network service provider.)	

1 Monthly and yearly price for the above combinations of throughputs will be discovered.

25.2.4 Security Services

1) Hardware Security Module

Sr. No.	Service Name	Service Definitions	Service Procurement Parameter[2]	
			No. of Dedicated HSM Required	Number of RSA 2048-bit Key Generation Per 10 Seconds
1	Cloud Based Hardware Security Module (HSM)	This service can be used where a dedicated hardware security module is required to create, manage and control keys. The HSM must comply with FIPS 140-2 Level 3 requirements.	Choose an item.	Choose an item.

[2] Hourly, monthly and yearly price per dedicated HSM will be discovered for each of the performance categories (number of RSA 2048-bit key generation per 10 seconds).

2) Distributed Denial of Services

Sr. No.	Service Name	Service Definition	Service Procurement Parameter[1]	
			No. of Public IPs to be Protected	Amount of Outbound Data Transfer (TB)

Sr. No.	Service Name	Service Definition	Service Procurement Parameter[1]	
			No. of Public IPs to be Protected	Amount of Outbound Data Transfer (TB)
1	Distributed Denial of Service (DDoS)	This service can be used to protect various resources within the Cloud environment of CSP against malicious attempt to disrupt normal traffic of a target, service or network by overwhelming the target or its surrounding infrastructure with a flood of internet traffic.	Choose an item.	Choose an item.

[1] Monthly price per Public IP to be protected and per GB of outbound data transfer will be discovered.

3) TLS / SSL Certificate Management

Sr. No.	Service Name	Service Definitions	Service Procurement Parameter	
			Type of Certificate	No. of Certificates[1]
1	TLS/SSL Certificate Management	This service may be used to request (create), manage, and deploy public and private SSL/TLS certificates in CSP's cloud environment. This service frees the user from the cumbersome process of buying, uploading, and renewing SSL/TLS	Choose an item.	Choose an item.

Sr. No.	Service Name	Service Definitions	Service Procurement Parameter	
			Type of Certificate	No. of Certificates[1]
		certificates.		

[1] For each type of certificate, price per certificate will be discovered for the above range of certificates.

4) Dual / Multifactor Authentication

Sr. No.	Service Name	Service Definitions	Service Procurement Parameter
			No. of Users
1	Dual /Multi Factor Authentication	This service may be used to protect the IT resources by providing an extra layer of security that requires not only a username and password but also other information that user of the service has. The service must provide capability to integrate with LDAP or other directory services.	Choose an item.

[1] For the above range of users, monthly and yearly price per user will be discovered.

25.2.5 Monitoring Services

1) Log Analysis

Sr. No.	Service Name	Service Definition	Service Procurement Parameter
			Amount of Data to be Analyzed (GB)[1]
1	Log Analyzer	This service may be used to generate insights from of the logs, by running queries against these logs. The service must retain the log for at least 30 days.	Choose an item.

[1] For the above range of data, monthly price per GBwill be discovered. The price includes the prices for data ingestion into the service, data retention and query execution. There not be any additional cost associated with availing this service.

2) Operational Metric Collection

Sr. No.	Service Name	Service Definition	Service Procurement Parameter	
			Type of Metric	Number of Metrics[1]
1	Operational Metric Collection	This service may be used to collect the operational metrics such as CPU utilization, memory utilization, etc., defined by the CSP. The service also allows Government	Custom	Choose an item.

Sr. No.	Service Name	Service Definition	Service Procurement Parameter	
			Type of Metric	Number of Metrics[1]
		Organizations to create their own custom metrics.		

[1] For above range of metrics, monthly price per metric will be discovered for both the types – Built-In and Custom.

3) Alarm Service

Sr. No.	Service Name	Service Definition	Service Procurement Parameter
			Number of Alerts[1]
1	Alarm Service	This service may be used to set threshold value for built-in (provided by CSP) and custom (defined by Government Organization) metrics. Once the threshold is reached, an alarm/alert will be triggered and necessary actions may be taken. *This service may be procured only when the "Operational Metric Collection" service is procured.	Choose an item.

[1] For the above range of alerts, monthly price per alert will be discovered.

4) Notification Service

Sr. No.	Service Name	Service Definition	Number of Notifications
1	Email Notification Service[1]	This service may be used to send email notifications to the target recipient when an alarm / alert is triggered and the corresponding notification is configured. * This service may be procured only when the "Alarm Service" is procured.	Choose an item.

[1] Monthl[1] Monthly price per 100000 emails will be discovered.y price per 100000 emails will be discovered.

2	SMS Notification Service[2]	This service may be used to send SMS notifications to the target recipient when an alarm / alert is triggered and the corresponding notification is configured. * This service may be procured only when the "Alarm Service" is procured.	Choose an item.

[2] For each of the ranges specified above, price per SMS will be discovered.

3	Voice Call Notification Service[3]	This service may be used to send voice call notifications to the target recipient when an alarm / alert is triggered and the	Choose an item.

Sr. No.	Service Name	Service Definition	Number of Notifications
		corresponding notification is configured. * This service may be procured only when the "Alarm Service" is procured.	

[3] For each of the ranges specified above, price per Voice Call will be discovered.

25.2.6 Office Productivity Suit

Sr. No.	Service Name	Service Definition	Service Procurement Parameter
			No. of Users[1]
1	Cloud based Enterprise Office Productivity Suit (COTS) – Microsoft Office 365	Microsoft Office 365	Choose an item.

[1] For the above range of users, monthly price per user shall be discovered.

Sr.	Service Name	Service Definition	Service Procurement Parameter

No.			No. of Users[1]
2	Cloud based Enterprise Open Source Office Productivity Suit	This service provides Office coverage for desktop, laptop, tablets and smart phones (Android, iOS and Windows) with per user subscription install rights. There is no need to pay for version upgrades; updates are included in the subscription along with new features rollout regularly.	Choose an item.

[1] For the above range of users, monthly price per user shall be discovered.

25.2.7 Analytics Services

1) Streaming Service

Sr. No.	Service Name	Service Definition	Service Procurement Parameter
1	Video Streaming Service	This service may be used to stream video from various devices located in Government Organization's premises and ingest them into the CSP's environment and provide storage, encryption and video indexing capabilities in real time and batch analysis mode.	To be specified by the CSPs

Sr. No.	Service Name	Service Definition	Service Procurement Parameter
2	Data Streaming Service	This service may be used to capture and store data from sources such as website clicks, social media activity, location tracking and other events.	To be specified by the CSPs

2) Massive Data Processing Service

Sr. No.	Service Name	Service Definition	Service Procurement Parameter
1	Massive Data Processing using Big Data Frameworks	This service may be used to process huge amount of data using frameworks such as Hadoop, Apache Spark, HBase, Presto, etc.	To be specified by the CSPs

3) Data Warehousing Service

Sr. No.	Service Name	Service Definition	Service Procurement Parameter
1	Data warehouse	This service may be used to host a central repository of information which acts as a single source of truth and which can be used to generate variety of reports and dashboards to assist in the decision making process.	To be specified by the CSPs

25.3 Managed Services

The Cloud Services mentioned under Basic and Advanced Cloud Services come with their associated managed services. However, if a Government Organization requires additional managed services, which are not provided as part of the Basic and Advanced Cloud services, they can procure those managed services separately as listed in this section. The managed services listed under this section are optional for CSPs to offer. These managed services have been listed below with a set of indicative inclusions which may change based on the individual Government Organization's requirements.

Since the scope of the managed services is very wide and vary from customers to customers, Government Organizations will discover the prices of the managed services, tailored to meet their unique requirements, on the GeM platform through the bid functionality available on it.

25.3.1 Disaster Recovery as a Service (DRaaS)

Sr. No.	Service Name	Service Definition	Service Procurement Parameter[1]
1	DRaaS (DC and DR both in the Cloud)	Under this service, Government Organizations will select the required Cloud Services at both DC and DR sites in Cloud, and specify the needed RPO and RTO. Service Inclusions: • Tools disaster recovery management and replication • During the change from DC-Cloud to DR-Cloud or vice-versa	Parameters may include RPO, RTO and actual scope of the work.

Sr. No.	Service Name	Service Definition	Service Procurement Parameter[1]
		(regular planned changes), there should not be any data loss. • There shall be asynchronous replication of data between DC-Cloud and DR-Cloud. • During normal operations, the DC-Cloud will serve the requests. The DR-Cloud site will not be performing any work but will remain on standby. • DC-Cloud Storage shall be replicated (Active-Active) on an ongoing basis at DR-Cloud site, as per the required RPO, RTO and replication strategy. • In the event of a site failover or switchover, DR-Cloud site will take over the active role, and all the requests will be routed through that site. • Application data and application states will be replicated between the two sites so that when an outage occurs, failover to the surviving DR-Cloud can be accomplished within the specified RTO. This is the period during which the compute environment for the application shall be equivalent to DC. The installed application instance and the database shall be usable and the same SLAs as DC-Cloud shall be provided. • The security at the DC-Cloud and DR-Cloud shall be same. • The CSP shall conduct DR drill once in every six months of operation wherein the DC-Cloud has to be deactivated and	

Sr. No.	Service Name	Service Definition	Service Procurement Parameter[1]
		complete operations shall be carried out from the DR-Cloud site. However, during the change from DC-Cloud to DR-Cloud or vice-versa (or regular planned changes), there should not be any data loss. • Automated switchover/ failover facilities (during DC-Cloud failure & DR Drills) to be provided • The switchback mechanism shall also be automated.	
2	DRaaS (Only DR in the Cloud)	Under this service, Government Organizations will select the required Cloud Services at the DR site in Cloud, and specify the needed RPO and RTO. Service Inclusions: • Tools disaster recovery management and replication • During the change from DC-Cloud to DR-Cloud or vice-versa (regular planned changes), there should not be any data loss. • There shall be asynchronous replication of data between DC-Cloud and DR-Cloud. • During normal operations, the DC-Cloud will serve the requests.	Parameters may include RPO, RTO and actual scope of the work.

Sr. No.	Service Name	Service Definition	Service Procurement Parameter[1]
		The DR-Cloud site will not be performing any work but will remain on standby. • DC-Cloud Storage shall be replicated (Active-Active) on an ongoing basis at DR-Cloud site, as per the required RPO, RTO and replication strategy. • In the event of a site failover or switchover, DR-Cloud site will take over the active role, and all the requests will be routed through that site. • Application data and application states will be replicated between the two sites so that when an outage occurs, failover to the surviving DR-Cloud can be accomplished within the specified RTO. This is the period during which the compute environment for the application shall be equivalent to DC. The installed application instance and the database shall be usable and the same SLAs as DC-Cloud shall be provided. • The security at the DC-Cloud and DR-Cloud shall be same. • The CSP shall conduct DR drill once in every six months of operation wherein the DC-Cloud has to be deactivated and complete operations shall be carried out from the DR-Cloud site. However, during the change from DC-Cloud to DR-Cloud or vice-versa (or regular planned changes), there should not be any data loss. • Automated switchover/ failover facilities (during DC-Cloud failure	

Sr. No.	Service Name	Service Definition	Service Procurement Parameter[1]
		& DR Drills) to be provided • The switchback mechanism shall also be automated.	

[1] Actual price will depend on the scope of the work.

25.3.2 Backup as a Service

Sr. No.	Service Name	Service Definition	Service Procurement Parameter[1]
1	Backup as a Service	This service may be used to back up virtual machines,storage volumes, file systems and databases within the CSP's own Cloud environment. Following activities are included under this service: monitoring, reporting, notifications/alerts & incident management, backup storage, scheduling & retention, restoration, backup data protection, etc. The backup service should support granular recovery of virtual machines, database servers, Active Directory including AD objects, etc. Government Organization should be able to recover individual files, complete folders, entire drive or complete system to source machine or any other machine available in network.	Parameters may include type of backup (full backup and incremental backup), frequency of backup (weekly, monthly, etc.), retentions period (7 days, 30 days, etc.) and actual scope of the work.

Sr. No.	Service Name	Service Definition	Service Procurement Parameter[1]
		The backup service must provide following capabilities. ▪ Compression: Support compression of data at source before backup • Encryption: Support at least 128 bit encryption at source ▪ Alert: Support email notification on backup job's success / failure ▪ File exclusion: Ability to exclude specific files, folders or file extensions from backup • Deduplication: Provide deduplication capabilities	

[1] Actual price will depend on the scope of the work.