

**Invitation for
Extending the Empanelment of Cloud
Service Offerings of Cloud Service
Providers (CSPs)**

Additional Requirements for CSPs

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

April' 2019

Table of Contents

| | |
|----------------------------------------------------------------------|-----------|
| 1. Background | 3 |
| 2. Purpose of the Invitation | 4 |
| 3. Cloud Services Empanelment Process for Existing CSPs | 5 |
| 4. Cloud Service Models..... | 7 |
| 5. Issuing Authority | 9 |
| 6. Modified / New Clauses..... | 10 |
| 7. Compliance Requirements..... | 21 |

1. Background

Ministry of Electronics & Information Technology (MeitY) conducted two rounds of empanelment of Cloud Service Providers (CSPs) in year 2016 and 2017 respectively. 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.

In order to further extend the empanelment of Cloud Service Offerings of CSPs, MeitY has published this invitation document containing additional requirements along with the revised clause(s) of the existing CSPs Empanelment RFP / Application Document. The existing CSPs Empanelment RFP / Application Document can be seen by visiting the following URL.

<https://meity.gov.in/writereaddata/files/Application%20for%20Empanelment%20of%20CSPs.pdf>

The CSPs whose Cloud Service Offerings are already empaneled with MeitY, will mandatorily be required to meet the additional requirements specified in this invitation document, in order to continue offering their services to government organizations in India. All other terms & conditions mentioned in the existing CSPs Empanelment RFP / Application Document remain the same.

2. Purpose of the Invitation

The primary purpose of this invitation document is to extend the empanelment of Cloud Service Offerings of CSPs and empanel any new Cloud Service Offerings of existing CSPs. MeitY shall carry out a separate process for new CSPs who wish to get their Cloud Service Offerings empaneled with MeitY.

The revised empanelment process allows CSPs to approach MeitY anytime for getting their services empaneled. The empanelment window will be open throughout the year. In the revised empanelment process, detailed audit of each CSP shall be conducted before its services are empaneled with MeitY. This audit shall be valid for a duration of three years. 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

MeitY invites applications from the CSPs (hereinafter referred to as “Applicants”) for extending empanelment of Cloud Service Offerings of CSPs and empaneling any new 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).

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”. 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.

This invitation document does not commit MeitY to enter into a binding agreement in respect of the project with the potential Applicants.

3. Cloud Services Empanelment Process for Existing CSPs

The complete process of Cloud Services Empanelment is as follows:

Step 1 - Cloud Service Details by CSP: The CSPs shall submit 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.

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 in a week’s time.
- (ii) STQC shall audit the Data Center(s) and Cloud Service Offerings of each CSP within a period of 6-8 weeks.
- (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 MeghRaj webpage available on the MeitY website.

- (i) In case of a successful audit by STQC, MeitY shall issue a Letter 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 deviations are found in the audit conducted by the STQC, the CSP shall be informed about this and advised to address these deviations and reapply for the empanelment.

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.

4. Cloud Service Models

As specified earlier, CSPs shall be required to offer their Cloud services as per the Cloud Services 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.

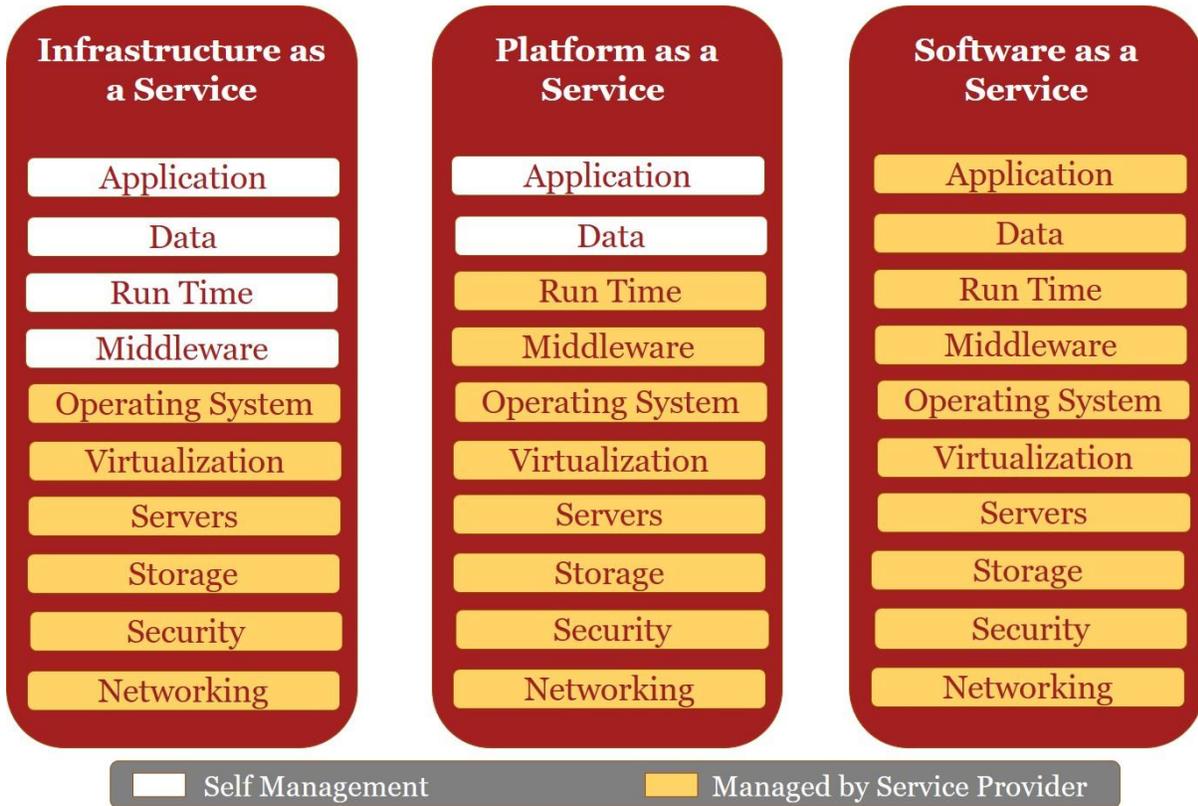


Figure 1: Cloud Service Models

- (i) **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. 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.
- (ii) **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.

(iii) 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.

5. Issuing Authority

The invitation for extending the empanelment of Cloud Service Offerings of CSPs is published by the Ministry of Electronics and Information Technology (MeitY). MeitY's decision with regard to the extension of empanelment of Cloud services through this application shall be final.

| S. No. | Item | Description |
|---------------------------------------------|------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 1 | Project Title | Invitation for Extending the 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 | Kshitij Kushagra Scientist E/Addl. Director Ministry of Electronics and Information Technology Electronics Niketan , 6, CGO Complex New Delhi-110 003 Tel: +91-11- 24301202 |
| 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 | Kshitij Kushagra Scientist E/ Addl. Director Room No. – 2002, 2 nd Floor Ministry of Electronics and Information Technology, Electronics Niketan , 6, CGO Complex New Delhi-110 003 Tel: +91-11- 24301202 |
| 7 | MeitY website | http://meity.gov.in/ |

6. Modified / New Clauses

The changes specified in the following table are with respect to the CSPs Empanelment RFP / Application Document available at the following URL.

<https://meity.gov.in/writereaddata/files/Application%20for%20Empanelment%20of%20CSPs.pdf>

| S. No | RFP Clause No. & Page No | RFP Clause | Modified / New Clause |
|-------|---------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 1. | Section 2, Purpose of the Application, Page No. 7 | MeitY invites applications / proposals from the Cloud Service Providers offering Cloud services (hereinafter referred to as “Applicants”) for empanelment of their Cloud Service Offerings for a combination of Deployment Models (Public Cloud, Virtual Private Cloud and Government Community Cloud). 1. Infrastructure as a Service (IaaS) 2. Platform as a Service (PaaS) 3. Disaster Recovery as a Service (DRaaS) 4. Dev / Test Environment as a Service (DevOps) 5. Virtual Desktop as a Service (VDaaS) | MeitY invites applications from the Cloud Service Providers (hereinafter referred to as “Applicants”) for empanelment of their Cloud Service Offerings across following Cloud Service Models: 1. Infrastructure as a Service (IaaS) 2. Platform as a Service (PaaS) 3. Software as a Service (SaaS) The CSPs may offer the services for a combination of the Deployment Models (Public Cloud, Virtual Private Cloud and Government Community Cloud). The CSPs shall be responsible to provide details of individual Cloud Services; and the Cloud Deployment Models and the Cloud Service Models under which these services shall be offered to government organizations. |
| 2. | Section 5, Compliance Requirements, Page No. 10 | The Cloud Service Offerings of the Cloud Service Provider (CSP) must comply with the below mandatory requirements to qualify for getting empaneled. In the scenario where one or a combination of IaaS, PaaS, DevOps and VDaaS Cloud service offerings of the Cloud Service | The Cloud Service Offerings of the Cloud Service Provider (CSP) must comply with the below mandatory requirements to qualify for getting empaneled. In the scenario where one or a combination of Cloud services of the CSP under IaaS, PaaS, |

| | | | |
|-----------|---------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| | | Provider (CSP) are proposed to be empaneled, the CSP also has the option to provide one or a combination of the managed services. | and SaaS are proposed to be empaneled, the CSP also has the option to provide one or a combination of the managed services. |
| 3. | New Clause Section 5.1, Deployment Model Specific Requirements, Page No. 16 | | Serial No. 29, as specified below, will be added in the table on page # 16. “CSP shall ensure that GCC environment is operational with a minimum of 5 numbers of 42U racks covering Compute, Storage, Network and Security components, for immediate use at the time of submission of application for empanelment.” |
| 4. | Section 5.2, General Requirements, Page No. 17, Point No. 11 | Should adhere to the relevant standards published (or to be published) by MeitY or any standards body setup / recognized by Government of India and notified to the CSP by MeitY as a mandatory standard. | CSPs need to adhere to all legal, statutory and regulatory requirements as notified by the Government of India from time to time. CSP shall not share data with any third party without explicit approval by the User Department, unless legally required to do so by the courts in India. If any new guidelines are published by MeitY which CSPs are required to adhere to, the CSPs shall be responsible for all costs associated with assessing, implementing, documenting and maintaining the empanelment. In case any misconduct is found, MeitY/ User department reserves the right to take appropriate legal course of action including blacklisting of the CSP. |
| 5. | Section 5.2, General | Government Department has the option to extend the | The empanelment window will be open throughout the year. In |

| | | | |
|------------------|-----------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| | <p>Requirements, Page No. 18, Point No. 15</p> | <p>Empanelment duration on expiry, to avail the services of the CSP for continuation of the services without the need to go for a separate empanelment process. The duration of extension will be decided by Government Department and will be up to a maximum of one year. The decision on the extension will be taken exclusively by Government Department keeping in consideration a) satisfactory performance of the Agency b) time constraints or other serious impediments in initiation c) technological reasons d) where circumstances inescapably require taking recourse to this option.</p> | <p>the new empanelment process, detailed audit of each CSP shall be conducted before its services are empaneled with MeitY. This audit shall be valid for a duration of three years. Thereafter, each CSP shall also undergo a surveillance audit every year for the following two requirements.</p> <ul style="list-style-type: none"> (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 <p>The decision on the extension of empanelment of Cloud Service Offerings of CSPs shall be taken exclusively by MeitY keeping in consideration (a) satisfactory performance of the CSP (b) time constraints or other serious impediments in initiation (c) technological reasons (d) where circumstances inescapably require taking recourse to this option.</p> |
| <p>6.</p> | <p>Section 5.3.4, Data Management, Page No. 21, Point No. 2</p> | <p>CSPs shall provide tools and mechanism to the Government Department or its appointed agency for defining their backup requirements & policy.</p> | <p>CSPs shall provide tools and mechanism 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.</p> |

| | | | |
|----|---------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 7. | Section 5.3.4, Data Management, Page No. 21, Point No. 4 | Transfer data back in-house either on demand or in case of contract or order termination for any reason | 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 |
| 8. | New Clause Section 5.7, Data Center Facility Requirements Page No. 23 & 24 | | Point No. 12, as specified below, will be added after Point No. 11 on page # 24. “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.” |
| 9. | Section 5.10, Disaster Recovery and Business Continuity Requirements, Page No. 27 & 28, Point No. 1 & 2 | 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. RPO should be less than or equal to 2 hours and RTO shall be less than or equal to 4 hours. The key transaction data shall have RPO of 15 minutes. However, during the change from Primary DC to DRC or vice-versa (regular planned changes), there should not be any data loss. There shall be asynchronous replication of data between Primary DC and DRDC and the CSP will be responsible for sizing and providing the DC-DR replication link so as to meet the RTO and the RPO 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. RPO should be less than or equal to 2 hours and RTO shall be less than or equal to 4 hours. The key transaction data shall have RPO of 15 minutes. <i>However, the User Department may seek more stringent RTO, RPO, or any other disaster recovery requirements as per their needs.</i> During the change from Primary DC to DR or vice-versa (regular planned changes), there should not be any data loss. There shall be asynchronous replication of data between Primary DC |

| | | | |
|------------|-----------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| | | 2. The Primary DC (of the Government Department) and the DRC should be in different seismic zones | and DRDC and the CSP will be responsible for sizing and providing the DC-DR replication link so as to meet the RTO and the RPO requirements. 2. The DC & DR sites shall be separated by a minimum distance of 100 kilometers. |
| 10. | New Clause Section 5.13, Management Reporting Requirements, Page No. 36 | | Point No. 9, as specified below, shall be added after the Point No.8. “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). MeitY shall provide the report template.” |
| 11. | New Clause Section 5.15.1, Backup Services, Page No. 37 | | Following points shall be added after the Point No. 2. 3. The CSP shall be responsible for back up of virtual machines, storage volumes, file systems, and databases within the CSP’s own Cloud environment. 4. CSP 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 |

| | | | |
|------------|---------------------------------------------------------------|--|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| | | | <p>minimum 30 days or as desired by the User Department as per their needs.</p> <p>6. The backup solution offered by CSP shall support granular recovery of virtual machines, database servers, Active Directory including AD objects, etc. User Department should be able to recover individual files, complete folders, entire drive or complete system to source machine or any other machine available in network.</p> <p>7. The backup service must provide following capabilities:</p> <ul style="list-style-type: none"> • 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 |
| 12. | New Section Technical requirements for “Software as | | Section “5.16. Technical requirements for “Software as a Service’ offerings”, as specified |

| | | |
|--|------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| | <p>a Service' offerings, Page No. 40</p> | <p>below, shall be added on Page No. 40.</p> <ul style="list-style-type: none"> (i) Cloud services under SaaS model shall only be offered from Data Centers audited and qualified by STQC under the Cloud Services Empanelment process. (ii) CSPs shall be responsible for ensuring that all data functions and processing are performed within the boundaries of India. (iii) CSPs shall be responsible to ensure that the services offered from SaaS provide a mechanism to authenticate and authorize users. (iv) SaaS solution / services offered to User Departments shall have in-built functionality to integrate with existing authentication mechanisms like Active-Directory. (v) SaaS solution shall be able to segregate users on basis of privileges granted to the users. (vi) CSPs shall provision and implement role-based authentication when required and separation of identities shall be maintained in multi-tenant environment. (vii) CSPs shall ensure that all the policies and procedures shall be |
|--|------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

| | | | |
|--|--|--|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| | | | <p>established and maintained in support of data security to include (confidentiality, integrity, and availability) across various system interfaces, business functions to prevent any improper disclosure, alternation, or destruction.</p> <p>(viii) CSPs shall ensure any service offered from SaaS are monitored, controlled and administered using web based tool with visibility to the User Department.</p> <p>(ix) CSPs shall ensure that User Departments are provided with capability to generate custom reports around several parameters such as users, time, data, etc.</p> <p>(x) 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.</p> <p>(xi) 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</p> |
|--|--|--|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

| | | | |
|-----------|-------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| | | | <p>performance requirements.</p> <p>(xii) CSPs shall ensure that any service offered from the SaaS solution provider comply with PII data security standards like ISO 27018.</p> <p>(xiii) CSPs shall ensure that services offered under SaaS are enabled with data loss prevention tools and capability to monitor data flow.</p> <p>(xiv) CSPs shall ensure that services offered under SaaS provide tools / capability for encryption of data-at-rest, data-in-processing and data-in-transit.</p> <p>(xv) CSPs shall ensure that services offered under SaaS support encryption algorithms like AES256 and higher.</p> |
| 13 | Section 9.4.b, Page No. 54 | In case of such a breach, MeitY will serve a thirty days written notice for curing this Breach. In case the breach continues, after the expiry of such notice period, the MeitY will have the option to terminate the Empanelment. | In case of such a breach, MeitY will serve a 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. |
| 14 | New Section De-Registration and De-Empanelment, Page No. 56 | <p>Point No. 12, as specified below, shall be added after the Point No. 11.</p> <p>“12. De-Registration and De-Empanelment</p> <p>a. The CSP shall be de-registered and its services shall be de-empanelled, under the following circumstances</p> <ul style="list-style-type: none"> i. If the CSP does not register on GeM platform within 30 days of empanelment. ii. If the CSP registers on GeM platform but doesn't list its empanelled Cloud Services on GeM platform in a period of 30 days from the date of empanelment. 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 <p>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</p> |

| | | | |
|--|--|--|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| | | | <p>MeitY and all the User Departments where the CSP is offering the said service, specifying the reason for applying for the de-empement. 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.”</p> |
|--|--|--|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

7. Compliance Requirements

CSPs are required to show their compliances to the requirements specified in Annexure 2. If a Data Center facility is owned by a CSP, the CSP shall be responsible to provide and submit the certification(s) in its name. If the CSP does not own a Data Center facility and has hosted its IT Infrastructure in a third party Data Center, the certifications requirements related to the Data Center facility shall be in the name of the facility owner but submitted by the CSP.

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

Annexure - 1

Application Response Cover Letter

Original signed copy on company letterhead

[Date]

To,

Mr. Kshitij Kushagra
Scientist E/Addl. Director
Ministry of Electronics and Information Technology
Electronics Niketan, 6, CGO Complex
New Delhi-110 003
Tel: +91-11- 24301202

Dear Sir,

Ref: Response to Invitation for Extending the Empanelment of Cloud Service Offerings of Cloud Service Providers

Having examined the invitation document, 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 the invitation document.
- 2 We hereby declare that all the information and statements in this application / 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 application / proposal that you may receive.

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:

Annexure - 2 Compliance Requirements

The Cloud Service Provider is required to fill the following table and submit a copy of each certificate mentioned in the table.

| Certification | Compliance (Yes /No) | Certificate Number | Issued To | Issued By | Issue Date | Expiration Date |
|-----------------------------|----------------------|--------------------|-----------|-----------|------------|-----------------|
| ISO 27001 | | | | | | |
| ISO 20000:1 | | | | | | |
| ISO 27017 | | | | | | |
| ISO 27018 | | | | | | |
| TIA - 942 (A/B) | | | | | | |
| / | | | | | | |
| UPTIME (Tier III or higher) | | | | | | |

Note: CSP shall be required to comply with Cloud Security ISO Standard ISO 27017:2015, Privacy Standard ISO 27018:2014

Annexure - 3
Acceptance to offer Basic Cloud Services as defined in
Cloud Services Bouquet of MeitY

(Original signed copy on the company letterhead)

[Date]

To,

Mr. Kshitij Kushagra
Scientist E/Addl. Director
Ministry of Electronics and Information Technology
Electronics Niketan, 6, CGO Complex
New Delhi-110 003
Tel: +91-11- 24301202

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:

Annexure - 4

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 Centre Facility Name & 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 | . | | | | | | | |
| 7 | . | | | | | | | |
| | Add as many rows as required | | | | | | | |

* All “Basic Cloud Services” as defined in the Cloud Services Bouquet 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 - 3.

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

Annexure - 5

Advanced Cloud Services Empanelment Form

| 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 & 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 | PostgreSQL | <Description> | Public Cloud | PaaS | No | Yes | Yes | |
| 2 | . | | | | | | | |
| 3 | . | | | | | | | |
| 4 | . | | | | | | | |
| 5 | . | | | | | | | |
| 6 | . | | | | | | | |
| 7 | . | | | | | | | |
| | Add as many rows as required | | | | | | | |

<<<End of the Invitation Document>>>