Guidelines for Government Departments On Contractual Terms Related to Cloud Services

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

March 31, 2017

This Page is Intentionally Left Blank

Table of Contents

This Page is Intentionally Left Blank

1. Background

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

1.1 Provisional Empanelment of Cloud Service Offerings

Taking demand into consideration, MeitY has initiated Provisional Empanelment of the cloud service offerings of Service providers that the end-user departments can leverage in addition to the National Cloud services offered by NIC for their e-governance solutions.

The following cloud service offerings offered by the Cloud Service Providers (http://meity.gov.in) for a combination of the Deployment Models (Public Cloud, Virtual Private Cloud and Government Community Cloud) have been provisionally empanelled by MeitY.

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 Desktops as a Service (VDaaS)

The provisional empanelment shall be initially for two years from the date of accepting the terms and conditions by the empanelled cloud service providers. The provisionally empanelled cloud service providers will have the option to comply with the full-fledged guidelines / standards to get the certification for their offerings as and when the new guidelines / standards are published by MeitY.

STQC is in the process of auditing and certification of the empanelled services. MeitY has opened up the process of empanelment and henceforth the potential Cloud Service Providers can apply for empanelment and certification by MeitY. The audited/certified service offerings of various CSPs are available at www://meity.gov.in

1.2 Guidelines for Procurement of Cloud Services

To further facilitate the end user departments in procuring/ adopting cloud computing services, MeitY has prepared broad guidelines highlighting key considerations that Government Departments need to be aware of when procuring cloud services. The guidelines also detail out the services and requirements that can be used when preparing the Request for Proposal (RFP) document.

In addition to the above, this document highlights the contractual terms/issues that may be considered by departments when formulating contracts for cloud procurement.

2. Critical Contractual Issues in Cloud Procurement

MeitY through the empanelment process has ensured that the cloud service offerings of the service providers (CSPs) comply with certain legal requirements. But the Government Departments need to be aware of certain critical areas that need to be addressed in cloud computing agreements. While broad guidelines are provided in this document, Departments should always carefully review and obtain all necessary legal advice on the specific terms to use. Also there may be certain significant issues that may be required for specific projects, for example, some issues relating to the protection of personal information may be not be important for projects that do not handle such data, where Departments may include other relevant clauses.

The critical issues that need to be addressed while formulating cloud contracts inter alia include:

2.1 Information Security

One of the most critical issues that need to be addressed in the Cloud Service Agreement is the security of the data. This issue further poses a significant risk if the data is sensitive in nature. The following contractual terms may be included in the agreements.

a. Certification/Compliance:

i. Departments need to ensure that the CSPs facilities/services are certified to be compliant to the following standards based on the project requirements:

- ISO 27001 - Data Center and the cloud services should be certified for the latest version of the standards
- ISO/IEC 27017:2015-Code of practice for information security controls based on ISO/IEC 27002 for cloud services and Information technology

- ISO 27018 - Code of practice for protection of personally identifiable information (PII) in public clouds.
- ISO 20000-9-Guidance on the application of ISO/IEC 20000-1 to cloud services
- PCI DSS - compliant technology infrastructure for storing, processing, and transmitting credit card information in the cloud – This standard is required if the transactions involve credit card payments.

MeitY with the help of STQC is carrying out the audit and is in the process of certifying the service offerings of CSPs for the above three standards. Therefore the Departments may include the following clauses in the agreements.

ii. The CSP/Service Provider shall comply or meet any security requirements applicable to CSPs/Service Providers 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/Service Providers by MeitY as a mandatory standard

iii. The CSP/Service Provider shall meet all the security requirements indicated in the IT Act 2000, the terms and conditions of the Provisional Empanelment of the Cloud Service Providers and shall comply to the audit criteria defined by STQC

(The Departments may refer the Information Classification, National Information Security Policy and Guidelines, Ministry of Home Affairs (MHA) while choosing to deploy on cloud)

b. Privacy and Security Safeguards.

The Department may ensure that specific clauses pertaining to the following are included in to the contracts.

i. If the data is classified as very sensitive, the Departments may include a clause to ensure that the data is encrypted as part of a standard security process for highly sensitive content or choose the right cryptographic algorithms evaluating security, performance, and compliance requirements specific to their application and may choose from multiple key management options.

ii. The Department may include a clause that the provider notifies the agency promptly in the event of security incidents or intrusions, or requests from foreign government agencies for access to the data, to enable the agency to manage these events proactively.

iii. At the end of the agreement, the Department shall ensure that all the storage blocks or multiple copies of data if any are unallocated or zeroed out by the CSPs so that data cannot be recovered. If due to some regulatory reasons if it is

required to securely decommission data, departments can implement data encryption at rest using departments managed keys, which are not stored in the cloud. Then customers may delete the key used to protect the decommissioned data, making it irrecoverable.

iv. The CSP/Service Provider shall report forthwith in writing of information security breaches to the Department by unauthorized persons (including unauthorized persons who are employees of any Party) either to gain access to or interfere with the Project's Data, facilities or Confidential Information.

v. The CSP undertakes to treat information passed on to them under this Agreement as classified. Such Information will not be communicated / published / advertised by the CSP to any person/organization without the express permission of the Department.

c. Confidentiality

In cases where the CSP has access to **highly sensitive information (in case of departments like defense)**, Departments may include the following clause in the agreements:

i. The CSP/Service Provider shall execute non-disclosure agreements with the Department with respect to this Project. For the avoidance of doubt, it is expressly clarified that the aforesaid provisions shall not apply to the following information:

- information already available in the public domain;
- information which has been developed independently by the Service Provider;
- information which has been received from a third party who had the right to disclose the aforesaid information;
- Information which has been disclosed to the public pursuant to a court order.

ii. The Subcontractors will be permitted to obtain customer data only to deliver the services the CSP has retained them to provide and will be prohibited from using customer data for any other purpose. The CSP remains responsible for its subcontractors' compliance with CSP's obligations under the Project."

d. Location of Data

The location of the data could be located in one or more discrete sites in foreign countries. Therefore it has to be specifically mentioned in the agreement. The terms

and conditions of the Empanelment of the Cloud Service Provider has taken care of this requirement by stating that all services including data will be guaranteed to reside in India. Therefore the following clause should be included in the contract:

i. The location of the data (text, audio, video, or image files, and software (including machine images), that are provided to the CSP for processing, storage or hosting by the CSP services in connection with the Department's account and any computational results that a Department or any end user derives from the foregoing through their use of the CSP's services) shall be as per the terms and conditions of the Empanelment of the Cloud Service Provider.

e. **E-Discovery:** Electronic discovery (e-discovery) is the process of locating, preserving, collecting, processing, reviewing, and producing Electronically Stored Information (ESI) in the context of or criminal cases/proceedings or investigation. The Department must be able to access and retrieve such data in a CSP environment in a timely fashion for normal work purposes.

f. **Law Enforcement Request:** The Law Enforcement Agency as mandated under any law for the time being in force may seek access to information stored on cloud as provided by the Service Provider. The onus shall be on the Service Provider to perform all due diligence before releasing any such information to any such law enforcement agency.

2.2 Audit

In the traditional Information Technology agreements, under the Article – Audit, Access and Reporting, clauses related to carrying out inspection and auditing are usually included to ensure compliances by the Service Provider. However, as the cloud services are provided to multitude of customers, the CSPs do not permit access to ensure security for all customers. Therefore Departments can check compliances by accessing and verifying all the global compliance certification audit reports. In addition, the Departments shall mention the standards that the CSPs need to demonstrate compliance to the standards such as ISO 27001, ISO 27018 etc. rather than physical access and audits. As STQC/MeitY is carrying out the audit and certification of the cloud service offerings of various CSPs, the Departments shall ensure that the Cloud Service Provider's services offerings are audited and certified by STQC/MeitY. The Departments may include the following clauses in the Agreement:

i. The Cloud Service Provider's services offerings shall comply with the audit requirements defined under the terms and conditions of the Provisional Empanelment of the Cloud Service Providers (or STQC /MEITY guidelines as and when published).

ii. The Audit, Access and Reporting Requirements should be as per the terms and conditions of the Provisional Empanelment of the Cloud Service Provider.

2.3 Transitioning/Exit

Transitioning can be a critical issue and it is important for the Departments to include the following clauses in the agreement.

a. The 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 Department. Any cost for retaining the data beyond 45 days shall be paid to the Service Provider based on the cost indicated in the commercial quote.

b. The CSP shall be responsible for providing the tools for import / export of VMs & content and the MSP shall be responsible for preparation of the Exit Management Plan and carrying out the exit management / transition

<< Clauses related to the MSP>>

c. The MSP shall provide the Department or its nominated agency with a recommended exit management plan ("Exit Management Plan") or transition plan indicating the nature and scope of the CSP's transitioning services. The Exit Management Plan shall deal with the following aspects of the exit management in relation to the Agreement as a whole or the particular service of the Agreement:

   i. Transition of Managed Services

   ii. Migration from the incumbent cloud service provider's environment to the new environment

d. The MSP is responsible for both Transitions of the Services as well as Migration of the VMs, Data, Content and other assets to the new environment.

e. The MSP shall carry out the migration of the VMs, data, content and any other assets to the new environment created by the Department or any other Agency (on behalf of the Department) on alternate cloud service provider's offerings to enable successful deployment and running of the Government Department's solution on the new infrastructure.

f. The format of the data transmitted from the cloud service provider to the new environment created by the Department or any other Agency should leverage standard data formats (e.g., OVF…) whenever possible to ease and enhance portability. The format will be finalized by the Government Department.

g. Transitioning from the CSP including retrieval of all data in formats approved by Department

h. The MSP shall ensure that all the documentation required by the Department for smooth transition (in addition to the documentation provided by the Cloud Service Provider) are kept up to date and all such documentation is handed over to the Department during regular intervals as well as during the exit management process.

i. The MSP will transfer the organizational structure developed during the Term to support the delivery of the Exit Management Services. This will include:

    i. Document, update, and provide functional organization charts, operating level agreements with Third-Party contractors, phone trees, contact lists, and standard operating procedures.

    ii. Transfer physical and logical security processes and tools, including cataloguing and tendering all badges and keys, documenting ownership and access levels for all passwords, and instructing Department or its nominee in the use and operation of security controls.

j. Some of the key activities to be carried out by MSP for knowledge transfer will include:

    i. Prepare documents to explain design and characteristics.

    ii. Carry out joint operations of key activities or services.

    iii. Briefing sessions on process and process Documentation.

    iv. Sharing the logs, etc.

    v. Briefing sessions on the managed services, the way these are deployed on cloud and integrated.

    vi. Briefing sessions on the offerings (IaaS/PaaS) of the cloud service provider

k. Transfer know-how relating to operation and maintenance of the software and cloud services.

2.4 Performance Management

Service levels are an important way of ensuring that a provider meets the level of service expected by the agency. The Departments may refer to - Guidelines on Service Level Agreement – that lists out the critical SLAs for cloud services.

2.5 Payment Terms

The monthly payments may be made at the end of each month based on the actual usage of the services and as per the “Unit Costs” under the commercial quote.

2.6 Dispute Resolution

It is important to be clear about how disputes in relation to the cloud computing agreement will be resolved. Departments should ensure that, at a minimum, the agreement states what country's (and jurisdiction's) laws apply to the agreement, which courts can hear disputes about the agreement and whether alternative dispute resolution mechanisms such as arbitration are proposed. Following clauses on Dispute Resolution may be incorporated:

a. Any dispute arising out of or in connection with this Agreement or the SLA shall in the first instance be dealt with in accordance with the escalation procedure as set out in the Agreement.

b. In case the escalations do not help in resolution of the problem within 3 weeks of escalation, both the parties should agree on a mediator for communication between the two parties. The process of the mediation would be as follows:

   i. Aggrieved party should refer the dispute to the identified mediator in writing, with a copy to the other party. Such a reference should contain a description of the nature of the dispute, the quantum in dispute (if any) and the relief or remedy sought suitable.

   ii. The mediator shall use his best endeavors to conclude the mediation within a certain number of days of his appointment.

   i. If no resolution can be reached through mutual discussion or mediation within 30 days then the matter should be referred to Experts for advising on the issue.

c. In case the mediation does not help in resolution and it requires expertise to understand an issue, a neutral panel of 3 experts, agreeable to both parties should be constituted. The process of the expert advisory would be as follows:

   ii. Aggrieved party should write to the other party on the failure of previous alternate dispute resolution processes within the timeframe and requesting for expert advisory. This is to be sent with a copy to the mediator.

   iii. Both parties should thereafter agree on the panel of experts who are well conversant with the issue under dispute

   iv. The expert panel shall use his best endeavors to provide a neutral position on the issue.

   v. If no resolution can be reached through the above means within 30 days then the matter should be referred to Arbitration.

d. Any dispute or difference whatsoever arising between the parties to this Agreement out of or relating to the construction, meaning, scope, operation or

effect of this Agreement or the validity of the breach thereof shall be referred to a sole Arbitrator to be appointed by mutual consent of both the parties herein. If the parties cannot agree on the appointment of the Arbitrator within a period of one month from the notification by one party to the other of existence of such dispute, then the Arbitrator shall be appointed by the High Court where the Department is located in India. The provisions of the Arbitration and Conciliation Act, 1996 will be applicable and the award made there under shall be final and binding upon the parties hereto, subject to legal remedies available under the law. Such differences shall be deemed to be a submission to arbitration under the Indian Arbitration and Conciliation (Amendment) Act 2015 or of any modifications, Rules or re-enactments thereof. The Arbitration proceedings will be held at the High Court where the Department is located in India. Any legal dispute will come under the sole jurisdiction of state jurisdiction of the Department in India.