TENDER DOCUMENT FOR

SELECTION OF MANAGED SERVICE PROVIDER/CLOUD SERVICE PROVIDER FOR PROVIDING CLOUD SERVICES FOR HOSTING ALL THE APPLICATIONS/WEBSITES PRESENTLY HOSTED IN THE MANIPUR SDC

DEPARTMENT OF INFORMATION TECHNOLOGY
GOVERNMENT OF MANIPUR
4TH FLOOR, WEST BLOCK
NEW SECRETARIAT, IMPHAL, MANIPUR

BID SUBMISSION DETAILS:

SL.	Particulars	Description
1	Last Date & Time for submission of bid	20th April, 2018 till 12.00 Noon
2	Date & Time of opening of Technical bid	23rd April, 2018 at 12.30 PM
3	Technical Presentation	24th April, 2018 at 11.00 AM
4	Date & Time of opening of Financial bid	Will be notified later.
5	Place of submission & opening of Bids	Department of Information Technology, Government of Manipur, 4th Floor, Western Block, New Secretariat , Imphal – 795001

TABLE OF CONTENTS

1. INTRODUCTION

Under National e-Governance Plan Scheme of Government of India, Manipur State Data Centre (SDC) as one of the core infrastructure components under National e-Governance Plan (NeGP) to consolidate services, applications and infrastructure to provide efficient electronic delivery of G2G, G2C and G2B services. Manipur State Data Centre (MSDC) was set up in Ground Floor, West Block New Secretariat Building Imphal to act as a central repository of all data and applications/websites for the entire Government of Manipur. 12 (Twelve) nos. of websites are presently hosted at the Manipur SDC. 5 (five) nos. of websites are in pipeline for hosting at the Manipur SDC.

e-District, CCTNS, SSDG,GSTN and NICNET Services are hosted in Co-location mode at MSDC. Manipur SDC is ISO-20000:2011 and ISO -27001:2013 certified and IPV6 enabled.

2. SCOPE OF WORK

DIT, Manipur wishes to engage a Managed Cloud Service Provider (MCSP)/Cloud Service Provider (CSP) for providing Cloud Services for a period of 3years, which may be reviewed for extension on the completion of third year at the discretion of DIT, Manipur to continue the hosting of all the applications/websites in the cloud platform .The Details of the websites and applications are at **Annexure-I**. The scope of work is as under:

2.1. Environment Requirement:

i. Infrastructure as Service (IaaS) for migration of all the applications/websites at **Annexure-C** and hosting of applications/websites for various Departments of Government of Manipur in future.

ii. The proposed Environment for the deployment of applications/websites at **Annexure-C** and hosting of applications/websites for various Departments of Government of Manipur in future are:
   a. Staging environment
   b. Production

iii. The above environments are to be deployed on the Cloud Platform.

iv. Each of the environments mentioned above should be logically isolated, i.e. the Staging environment should be in a different VLAN than the production environment and setup should be such that users of the environments are in separate networks.

v. The Bidder shall be responsible for provisioning required compute infrastructure (server/virtual machines), storage as the indicative compute requirements in the commercial Bid, in built Anti-Spam/Malware/Antivirus threats control software etc.

2.2 Migration of existing applications:

a. Migration of existing applications will be responsibility of DIT/Application Vendor.

b. CSP will support the migration process including VM configuration, Installation and configuration of OS, Network and VLAN Zone creation and configuration etc.

2.3 Operations & Maintenance Services

a. Resource Management

i. Adequately size the necessary compute, memory, and storage required, building the redundancy into the architecture (including storage) and load balancing to meet the service levels.

ii. While the initial sizing & provisioning of the underlying infrastructure may be carried out based on the information provide in the **Annexure-C.** Subsequently, it is expected that the CSP, based on the growth in the user load (peak and non-peak periods; year-on-year increase), will scale up or scale down the compute, memory, and storage as per the performance requirements of the solution.

iii. For any major expected increase in the workloads, carry out the capacity planning in advance 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. Range of Upward Auto-Scaling is 70% CPU utilisation.

iv. The scaling up / scaling down (beyond the auto-scaling limits or whenever the auto-scaling limits have to be changed) has to be carried out with prior approval by the DIT, Manipur. The Service Provider shall provide the necessary details including the sizing calculations, assumptions, current workloads & utilisations, expected growth / demand and any other details justifying the request to scale up or scale down.

b. Patch & Configuration Management

i. Manage the instances of storage, compute instances, and network environments. This includes department-owned & installed operating systems and other system software that are outside of the authorisation boundary of the CSP. Service Provider is also responsible for managing specific controls relating to shared touch points within the security authorisation boundary, such as establishing customised security control solutions. Examples include, but are not limited to, configuration and patch management, vulnerability scanning, disaster recovery, and protecting data in transit and at rest, host firewall management, managing credentials, identity and access management, and managing network configurations.

c. User Administration

i. Management of user in the OS level and firewall level will be take care by CSPs.

ii. Properly separates users by their identified roles and responsibilities, thereby establishing least privilege and ensuring that users have only the permissions necessary to perform their assigned tasks.

d. Security Administration

i. Appropriately configure the security groups in accordance with the DIT, Manipur networking policies.

ii. Regularly review the security group configuration and instance assignment in order to maintain a secure baseline.

iii. Secure and appropriately segregate / isolate data traffic/application by functionality using DMZs, subnets etc.

iv. Ensure that the cloud infrastructure and all systems hosted on it, respectively, are properly monitored for unauthorised activity.

v. Properly implementing anti-malware and host-based intrusion detection systems on their instances, as well as any required network-based intrusion detection systems in accordance with the DIT, Manipur Security policies.

e. Monitoring Performance and Service Levels.

i. Provide and implement tools and processes for monitoring the availability of assigned applications, responding to system outages with troubleshooting activities designed to identify and mitigate operational issues.

ii. Reviewing the service level reports, monitoring the service levels and identifying any deviations from the agreed service levels.

iii. Monitoring of service levels, including availability, uptime, performance, application specific parameters, e.g. for triggering elasticity, request rates, number of users connected to a service.

iv. Detecting and reporting service level agreement infringements.

v. Monitoring of performance, resource utilisation and other events such as failure of service, degraded service, availability of the network, storage, database systems and operating Systems including API access within the cloud service provider's boundary.

f. Usage Reporting and Billing Management

i. Track system usage and usage reports
ii. Monitoring, managing and administering the monetary terms of SLAs and other billing related aspects
iii. Provide the relevant reports including real time as well as past data/information/reports to validate the billing and SLA related penalties
iv. Provide the Access Log report

g. Backup

i. Configure, schedule, monitor and manage backups of all the data including application and database but not limited to files, images and databases as per the policy finalized by DIT, Manipur.
ii. Restore from the backup where required.

h. Business Continuity Services

i. Provide business continuity services in case the primary site becomes unavailable.

i. Support for third party audits

i. Enable the logs and monitoring as required to support for third party audits.

j. Miscellaneous

i. Advise on optimal operational practices, recommend deployment architectures for cloud infrastructures, design and implement automated scaling processes, day-to-day and emergency procedures, deploy and monitor underlying cloud services, performance reporting and metrics, and ensure the overall reliability and responsive operation of the underlying cloud services through both proactive planning and rapid situational response.

2.4 Exit management / transition-out services

a. Provide a comprehensive exit management plan
b. Migration of the VMs, data, content and any other assets to the new environment or on alternate cloud service provider's offerings and ensuring successful deployment and running of the Government Department's solution on the new infrastructure by suitably retrieving all data, scripts, software, virtual machine images, and so forth to enable mirroring or copying to Department supplied industry standard media
c. Ensure that all the documentation required for smooth transition including configuration documents are kept up to date
d. Retain the data at the end of the agreement (for a maximum of 45 days beyond the expiry of the Agreement). If data is to be retained the cost for retaining the data may be obtained in the commercial quote.
e. Once the exit process is completed, remove the data, content and other assets from the cloud environment and destroy the VM, Content and data of the DIT Manipur.
f. Ensure that all the documentation required by the DIT, Manipur for smooth transition are kept up to date and all such documentation is handed over to the DIT, Manipur during regular intervals as well as during the exit management process.
g. Support and assist the DIT, Manipur for a period of three months so that the DIT, Manipur is able to successfully deploy and access the services from the new environment.
h. Train and transfer the knowledge to the DIT, Manipur team to ensure similar continuity and performance of the Services post expiry of the Agreement.

Note: The ownership of the data generated upon usage of the system, at any point of time during the contract or expiry or termination of the contract, shall rest absolutely with DIT, Manipur.

2.5 Technical Features:

a. Financial analysis recommendation engine

CSP must offer a service by which recommendations are made to the customer about configurations the customer can make to optimize their financial spend with the provider. The service must provider customer-specific recommendations based on current or historical patterns at the provider and must not be customer-generic. Recommendations must be actionable, tied to specific assets and documented as having a certain amount of financial savings. This service must be offered directly by the provider and not require the customer to seek third-party partners.

b. Content delivery network

CSP must offer a service for global content delivery networking. The CDN service must be offered in self-service fashion with all maintenance offered by the provider.

c. Hadoop as a service

Cloud Service Providers must offer a Hadoop environment that is provided for the customer as a fully automated self-service turnkey offering. This must be a full service, not simply a "one click install" of Hadoop or the like.

d. Relational DBaaS

Cloud Service provider must offer a relational database as a service (DBaaS), provided as a fully automated, self-service turnkey offering. In this service, the customer should not have access to the underlying instance, and the database maintenance must be done entirely by the provider. At a minimum, the service must support two open-source database (either MySQL and PostgreSQL) and two enterprise database (either Microsoft SQL Server and Oracle). CSP must offer relational DBaaS in a locally redundant fashion, meaning that the customer database is automatically replicated across multiple data centers within a single geography.

e. Local identity management and granular role-based authorization

Cloud Service Providers must include, at minimum, a local identity management system (that is, local accounts) with granular role-based authorization for network services in both the service interfaces and management console. At a minimum, the role-based authorization must support assigning authorization based on individual users and groups of users and delineation must be assignable per firewall, load balancer, IP address and network segment and support, as applicable, the following granular actions: create, delete and configure.

f. SIEM integration or service

CSP must offer out-of-the-box integration with leading SIEM products or provide a self-service, turnkey offering by which customers can configure real-time analysis and alerting of security events. At a minimum, the integration or service must support alerting, log retention and some form of forensic analysis that is able to search across logs and periods of time for patterns.

g. Customer VPN connectivity

CSP must allow customers to access the cloud service via an IPsec VPN tunnel or Secure Sockets Layer (SSL) VPN tunnel over the public Internet. This must be a self-service capability from the provider side, although customers will have to make configurations on their end.

h. Encryption services

The block and object storage services must offer self-service ability from both management console and Command Line Interface to opt into provider-enabled server side encryption (SSE) for objects or object hierarchies within the storage service.

i. Bulk data import/export with encryption

CSP must provide a portable storage device for bulk data import/export. Customer must be able to encrypt the data prior to transport and then decrypt it upon arrival. The encryption service must be built into the storage device and not left to the customer.

Annexure-C

Sl.	Domains name	Operating System	Database	Web Server	Application Server	Zoomla Version	WordPress-Version	PHP
1	dipr-manipur.gov.in	RHEL 5.7	MySQL 5.5.53	Apache/2.2.3	NA	2.5	NA	PHP 5.3.3
2	ldhcl.nic.in	RHEL 5.7	MySQL 5.5.53	Apache/2.2.3	NA	NA	4	PHP 5.3.3
3	yasmanipur.gov.in	RHEL 5.7	MySQL 5.5.53	Apache/2.2.3	NA	NA	3.8	PHP 5.3.3
4	ditmanipur.gov.in	RHEL 5.7	MySQL 5.5.53	Apache/2.2.3	NA	NA	4.2.4	PHP 5.4.10
5	agrimanipur.gov.in	RHEL 5.7	MySQL 5.5.53	Apache/2.2.3	NA	NA	3.9.3	PHP 5.3.3
6	rdmanipur.gov.in	RHEL 7.4	MySQL 5.5.53	Apache/2.4.6	NA	NA	4.7.4	PHP 5.4.16
7	manipurforest.gov.in	RHEL 6.7	MySQL 5.5.53	Apache/2.2.15	NA	3.4	NA	PHP 5.5.2
8	cmmanipur.gov.in	RHEL 7.4	MySQL 5.5.53	Apache/2.4.6	NA	NA	4.7.3	PHP 5.4.16
9	artnculturemanipur.gov.in	RHEL 7.4	MySQL 5.5.53	Apache/2.4.6	NA	NA	4.8	PHP 5.4.16
10	mtu.ac.in	RHEL 7.4	MySQL 5.5.53	Apache/2.4.6	NA	NA	4.8	PHP 5.4.16
11	ayushmanipur.gov.in	RHEL 7.4	MySQL 5.5.53	Apache/2.4.6	NA	NA	4.7.4	PHP 5.4.16
12	msits.gov.in	Win Server 2008 R2	MSSQL 2008R2	IIS 7.5.7600	NA			
13	ecabinetmanipur.gov.in	RHEL 7.4	Postgresql 9.2	Tomcat 8.5.15	NA			Java 1.8
14	eservicemanipur.gov.in	Red Hat Enterprise Linux 6.4 64 Bit	IBM DB2 Version 10.5	IBM HTTP Server	IBM Websphere Application Server version 8.5	N/A	N/A	Java 1.6
15	manipurportal.mn.gov.in	CentOS Linux 5.5	Postgresql 8.2	Apache/2.4.6	Jboss, Alferesco Community Edition	N/A	N/A	Java 1.6
16	mnpcitizenportal.gov.in	Oracle Solaris version- 11	My SQL 5.5	Glassfish Application Server 2.1u1	Oracle iPlanet WebServer 7.0/Sun Java System Directory Server 6.3	N/A	N/A	

Note:

i. All the different version of RHEL can be updated to RHEL 7.4 except RHEL 6.4 of eservicesmanipur.gov.in.
ii. Apache versions can be update to Apache 2.4.6.

3. <u>Commercial Bid-Pricing Summary Sheet</u>:

SL. (1)	Description (2)	Total cost excluding of taxes and other duties (3)	Total applicable taxes and all other duties (4)	Total amount (INR) 5=3+4 (5)
A.	**One Time Cost**			
i.	Cloud Services-Setup Cost as per **Annexure-A1**			
ii.	Migration Service Charges for migration of applications/websites presently hosted at the Manipur SDC at Annexure-C as per **Annexure-A2**			
	Grand Total for one time cost (A)			
B.	**Variable/Recurring Cost**			
i.	Operation and Maintenance/Managed Services Cost for a period of 3 years for minimum indicative requirement as per **Annexure B1**			
ii.	Cloud Services-Cost for pre-production and production environment for 3 years minimum indicative value for minimum indicative requirement as per **Annexure-B2.**			
iii.	Cloud Services-Cost for pre-production and production environment for 3 years requirement along with Operation and Maintenance charges if any (on Demand Pricing) for additional indicative requirement as per **Annexure-B3**.			
	Grand Total for Variable/Recurring cost (B)			
C	**Total Cost for Commercial Evaluation (C) = (A) +(B)**			

<u>Note</u>:

i. The Cloud Service Cost at item **B.ii and B.iii** are only indicative for price discovery. The Payment shall be made only for actual pay per usage as per the relevant unit price of the selected bidder. Bidder shall also provide for any requirement above the indicated additional requirement at **Annexure-B3** at the unit rate of B(iii).

SL.	Description	Unit of Measurement for Pricing	Unit Price (excluding taxes and all other duties)	Quantity	Multiplication Factor	Total Price (excluding taxes and all other duties)	Total Applicable Taxes and all other duties	Total Price for Evaluation (Including taxes and all other duties)
1.	Cloud Services-Setup Cost	Per VM	To be Filled by the Bidder	8	1			

Note:

i. The Cloud Service Cost at item **B.ii and B.iii** are only indicative for price discovery. The Payment shall be made only for actual pay per usage as per the relevant unit price of the selected bidder. Bidder shall also provide for any requirement above the indicated additional requirement at **Annexure-B3** at the unit rate of B(iii).

SL.	Description	Unit of Measurement for Pricing	Unit Price (excluding taxes and all other duties)	Quantity	Multiplication Factor	Total Price (excluding taxes and all other duties)	Total Applicable Taxes and all other duties	Total Price for Evaluation (Including taxes and all other duties)
1.	Migration Service Charges for migration of applications/websites	Per website/Application	To be Filled by the Bidder	16	1			

Note:

i. The Cloud Service Cost at item **B.ii and B.iii** are only indicative for price discovery. The Payment shall be made only for actual pay per usage as per the relevant unit price of the selected bidder. Bidder shall also provide for any requirement above the indicated additional requirement at **Annexure-B3** at the unit rate of B(iii).

SL.	Description	Unit of Measurement for Pricing	Unit Price (excluding taxes and all other duties)	Quantity	Multiplication Factor	Total Price (excluding taxes and all other duties)	Total Applicable Taxes and all other duties	Total Price for Evaluation (Including taxes and all other duties)
1.	Operation and Maintenance/Managed Services	Per VM per Month	To be Filled by the Bidder	8	1*12*3 Months			

Note:

The Cloud Service Cost at item **B.ii and B.iii** are only indicative for price discovery. The Payment shall be made only for actual pay per usage as per the relevant unit price of the selected bidder. Bidder shall also provide for any requirement above the indicated additional requirement at **Annexure-B3** at the unit rate of B(iii).

Annexure B2-Commercial Bid- Breakup of Cloud Services–(Minimum /Indicated Quantity for 12*3 months only for better price discovery purpose):

SL.	Description	Unit of Measurement for Pricing	Unit Price (excluding taxes and all other duties)	Quantity	Multiplication Factor	Total Price (excluding taxes and all other duties)	Total Applicable Taxes and all other duties	Total Price for Evaluation (Including taxes and all other duties)
		(1)	(2)	(3)	(4)	(5)=(2)*(4)	(6	(7)=(5)+(6)
Virtual Machines (4 Core CPU and 16 GB RAM)								
1.	4*16	Per Month	To be Filled by the Bidder	8 VMs	8*12*3 Months			
Storage (200 GB internal storage for Virtual Machines and 4000 GB storage for backup)								
2.	Storage for VM 100GB	Per GB per Month	To be Filled by the Bidder	3 VMs	3*200*12*3 Months			
3.	Storage for VM 200 GB	Per GB per Month	To be Filled by the Bidder	3 VMs	3*100*12*3 Months			
4.	Storage for VM 500 GB	Per GB per Month	To be Filled by the Bidder	2 VMs	2*500*12*3 Months			
5.	Backup Storage (DR Site)	Per GB per Month	To be Filled by the Bidder	500GB	4000*12*3 Months			
6.	Throughput (Minimum 5mbps speed)	Per GB per Month	To be Filled by the Bidder	1GB	1*12*3 Months			
Additional Services								
7.	VLAN (Minimum Nos. of 3 nodes)	Per VLAN per Month	To be Filled by the Bidder	3	3*12*3 Months			
8.	Back up (onsite DC)	Per GB per month	To be Filled by the Bidder	500	500*12*3 Months			
9.	Advanced DDOS enabled link	Per link per month	To be Filled by the Bidder	1	1*12*3 Months			
10.	Cost of retention of data beyond 45 days.	Per 100GB per month	To be Filled by the Bidder	500	1*12*3 Months			
11.	DNS Manager per DNS per month	Per instance/service per month	To be Filled by the Bidder	1	1*12*3 Months			

12.	Content Delivery Network	Per 100 GB per month	To be Filled by the Bidder	1	1*12*3 Months			
13.	IPSec VPN Connections	Per 10 connection per month	To be Filled by the Bidder	1	1*12*3 Months			
14.	Virtual Firewall – Instance Level & Subnet Level	Per instance/service per month	To be Filled by the Bidder	1	1*12*3 Months			
15.	Anti-virus	Per VM per Month	To be Filled by the Bidder	8	1*12*3 Months			
14.	Web Application Firewall (Layer 7)	Per instance/service per month	To be Filled by the Bidder	1	1*12*3 Months			
16.	Identity and Access Management	Per instance/service per month	To be Filled by the Bidder	1	1*12*3 Months			
17.	Managed Threat Detection Service	Per instance/service per month	To be Filled by the Bidder	1	1*12*3 Months			
18.	Security Incident Monitoring Services	Per instance/service per month	To be Filled by the Bidder	1	1*12*3 Months			
19.	Cloud management & monitoring tool per dashboard – Service Health Dashboard	Per instance/service per month	To be Filled by the Bidder	1	1*12*3 Months			
20.	Audit Trail – Includes Network & Access Logs	Per Audit per month	To be Filled by the Bidder	1	1*12*3 Months			

AnnexureB3 -Commercial Bid- Breakup of Cloud Services–On-Demand pricing:

SL.	Description	Unit of Measurement for Pricing	Unit Price (excluding taxes and all other duties)	Multiplication Factor	Total Price (excluding taxes and all other duties)	Total Applicable Taxes and all other	Total Price for Evaluation (Including taxes and all other
		(1)	(2)	(3)	(4)=(2)*(3)	(5)	(6)=(4)+(5)
Virtual Machines (4 Core CPU and 16 GB RAM)							
1.	4*16	Per VM per Month	To be Filled by the Bidder	12*1 Months			
2.	Storage for VM	Per 100 GB per Month	To be Filled by the Bidder	12*1 Months			
3.	Offside Backup Storage (DR Site)	Per 100GB per Month	To be Filled by the Bidder	12*1 Months			
4.	Throughput (Minimum 5mbps speed)	Per GB per Month	To be Filled by the Bidder	12*1 Months			
Additional Services							
5.	Operation and Maintenance charge	Per VM per Month	To be Filled by the Bidder	12*1 Months			
5.	VLAN (Minimum Nos. of 3 nodes)	Per VLAN per Month	To be Filled by the Bidder	12*1 Months			
6.	DC Back up (onsite DC)	Per 100 GB per Month	To be Filled by the Bidder	12*1 Months			
7.	Advanced DDOS enabled link	Per link per month	To be Filled by the Bidder	12*1 Months			
8.	Cost of retention of data beyond 45 days.	Per 100GB per month	To be Filled by the Bidder	12*1 Months			
9.	DNS Manager per DNS per month	Per instance/service per month	To be Filled by the Bidder	12*1 Months			

10.	Content Delivery Network	Per 100 GB per month	To be Filled by the Bidder	12*1 Months			
11.	IPSec VPN Connections	Per 10 connection per month	To be Filled by the Bidder	12*1 Months			
12.	Virtual Firewall – Instance Level & Subnet Level	Per instance/service per month	To be Filled by the Bidder	12*1 Months			
13.	Anti-virus	Per VM per Month	To be Filled by the Bidder	12*1 Months			
14.	Web Application Firewall (Layer 7)	Per instance/service per month	To be Filled by the Bidder	12*1 Months			
15.	Identity and Access Management	Per instance/service per month	To be Filled by the Bidder	12*1 Months			
16.	Server Side Encryption of data at rest	Per 100 GB per month	To be Filled by the Bidder	12*1 Months			
17.	Managed Threat Detection Service	Per instance/service per month	To be Filled by the Bidder	12*1 Months			
18.	Security Incident Monitoring Services	Per instance/service per month	To be Filled by the Bidder	12*1 Months			
19.	Cloud management & monitoring tool per dashboard – Service Health	Per instance/service per month	To be Filled by the Bidder	12*1 Months			
20.	Audit Trail – Includes Network & Access Logs	Per Audit per month	To be Filled by the Bidder	12*1 Months			

4. **Technical Parameter (70 marks)**

   a. **Past experience:** Numbers of years since the CSP started offering Cloud Services in India / Globally **– (Total – 10 marks)**

   b. **Capability to provide Auto Scaling feature – (Total – 10 marks)**

   c. **No of Capabilities to monitor the provisioned cloud services support by CSP (Total - 10 marks)**

      i. Visibility into the performance and availability of the cloud services being used, as well as alerts that are automatically triggered by changes in the health of those services.

      ii. Event-based alerts, to provide proactive notifications of scheduled activities, such as any changes to the infrastructure powering the cloud resources

      iii. System-wide visibility into resource utilization, application performance, and operational health through proactive monitoring (collect and track metrics, collect and monitor log files, and set alarms) of the cloud resources.

      iv. Capture logs of all user activity within an account. The recorded information should include the identity of the API caller, the time of the API call, the source IP address of the API caller, the request parameters, and the response elements returned by the cloud service. This is required to enable security analysis, resource change tracking, and compliance auditing.

      v. Ability to discover all of the provisioned resources and view the configuration of each. Notifications should be triggered each time a configuration changes, and departments should be given the ability to dig into the configuration history to perform incident analysis.

      vi. Monitoring of cloud resources with alerts to customers on security configuration gaps such as overly permissive access to certain compute instance ports and storage buckets, minimal use of role segregation using identity and access management (IAM), and weak password policies.

      vii. Automated security assessment service to help improve the security and compliance of applications deployed on cloud by automatically assessing applications for vulnerabilities or deviations from best practices.

   d. **Availability of Managed Database services –**No of managed database services (e.g. Support for multiple types of databases – PostgreSQL, MySQL, MariaDB, Oracle and MS SQL Server etc.) by Cloud Service Provider - **(Total -10 marks)**

   e. **Availability of Managed Operating System services –**No of managed operating System services by CSP. **(Total -5 marks)**

   f. **Disaster Recovery Site/ High Availability Zone - (Total 10 Marks).**

   g. **Overall Presentation – Approach & quality - (Total 15 marks)**

4.1 Check List for Bidder

SL.	Criteria	Bidder response (enclose documentary proof applicable.)
1	**Past Experience:**	
	Numbers of years since the CSP started offering Cloud Services in India / Globally.	
2.	**Project implementation Plan /activity**	
	a) "To be" architecture with minimum resources. Submit a "To be" architecture. **b) No. of resource** Resource should have minimum 3 years' experience in Data Centre/cloud environment.	
3.	**No of Capabilities to monitor the provisioned cloud services :** i. Visibility into the performance and availability of the cloud services being used, as well as alerts that are automatically triggered by changes in the health of those services. ii. Event-based alerts, to provide proactive notifications of scheduled activities, such as any changes to the infrastructure powering the cloud resources. iii. System-wide visibility into resource utilization, application performance, and operational health through proactive monitoring (collect and track metrics, collect and monitor log files, and set alarms) of the cloud resources. iv. Capture logs of all user activity within an account. The recorded information should include the identity of the API caller, the time of the API call, the source IP address of the API caller, the request parameters, and the response elements returned by the cloud service. This is required to enable security analysis, resource change tracking, and compliance auditing. v. Ability to discover all of the provisioned resources and view the configuration of each. Notifications should be triggered each time a configuration changes, and departments should be given the ability to dig into the configuration history to perform incident analysis. vi. Monitoring of cloud resources with alerts to customers on security configuration gaps such as overly permissive access to certain compute instance ports and storage buckets, minimal use of role segregation using identity and access management (IAM), and weak password policies. vii. Automated security assessment service to help improve the security and compliance of applications deployed on cloud by automatically assessing applications for vulnerabilities or deviations from best practices.	

4.	**Availability of Managed Database services –** No of the database services (e.g. Support for multiple types of databases – PostgreSQL, MySQL, Maria DB, Oracle and MS SQL Server etc.) managed by CSP.	
5.	**Availability of Managed Operating System services** No. of operating System services managed by CSP.	
6.	**Disaster Recovery Site / High Availability Zone:** CSP should have DR sites in different seismic zones in India Or CSP should propose DC-DR from different physical locations, supporting active-active arrangement.	

5. Security and Statutory Requirements

5.1. Certification/Compliance:

a. The CSP/Bidder facilities/services need to be certified / compliant to the following standards based on the project requirements:
   i. ISO 27001 - Data Center and the cloud services should be certified for the latest version of the standards.
   ii. ISO/IEC 27017:2015-Code of practice for information security controls based on ISO/IEC 27002 for cloud services and Information technology.
   iii. ISO 27018 - Code of practice for protection of personally identifiable information (PII) in public clouds.
   iv. ISO 20000-9-Guidance on the application of ISO/IEC 20000-1 to cloud services.
   v. 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.

b. The CSP/Bidder shall comply or meet any security requirements applicable to CSPs/bidders published (or to be published) by Ministry of Electronics Information and Technology (MeitY), Government of India or any standards body setup / recognized by Government of India from time to time and notified to the CSP/Bidder by MeitY as a mandatory standard.

c. The CSP/Bidder 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.

5.2. Privacy and Security Safeguards:

a. CSP/Bidder 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.

b. CSP/Bidder to notify 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.

c. The Bidder 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.

d. The CSP/Bidder shall report forthwith in writing of information security breaches to the DIT, Manipur 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.

e. 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 DIT, Manipur.

5.3. Confidentiality

1. The Bidder shall execute non-disclosure agreements with the DIT, Manipur with respect to migration and hosting of all the applications/websites. For the avoidance of doubt, it is expressly clarified that the aforesaid provisions shall not apply to the following information:

i. information already available in the public domain;
ii. information which has been developed independently by the Service Provider;
iii. 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.

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

5.4. Location of Data:

a. The Bidder shall be guaranteed that all services including data will reside in India.

b. The location of the data (text, audio, video, image files, drawing files, GIS files, pdf, and any compressed data and software (including machine images), that are provided to the CSP for processing, storage or hosting by the CSP services in connection with the DIT Manipur's account and any computational results that an DIT Manipur 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.

5.5 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. DIT, Manipur must be able to access and retrieve such data in a CSP environment in a timely fashion for normal work purposes.

5.6. 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 Cloud Service Provider to perform all due diligence before releasing any such information to any such law enforcement agency.

5.7. Audit:

a. DIT, Manipur shall ensure that the Cloud Service Provider's services offerings are audited and certified by STQC/MeitY.

b. 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).

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

5.8. Performance Management:

The critical SLAs for cloud services are covered under Section 5.11.

5.9. Audit and Governance Requirements

a. The CSP shall implement the audit & compliance features to enable the Agency to monitor the provisioned resources, performance, resource utilization, and security compliance:

b. View into the performance and availability of the cloud services being used, as well as alerts that are automatically triggered by changes in the health of those services.

c. Event-based alerts, to provide proactive notifications of scheduled activities, such as any changes to the infrastructure powering the cloud resources.

d. System-wide visibility into resource utilization, application performance, and operational health through proactive monitoring (collect and track metrics, collect and monitor log files, and set alarms) of the cloud resources.

e. Review of auto-scaling rules and limits.

f. Logs of all user activity within an account. The recorded information should include the identity of the API caller, the time of the API call, the source IP address of the API caller, the request parameters, and the response elements returned by the cloud service. This is required to enable security analysis, resource change tracking, and compliance auditing.

g. Ability to discover all of the provisioned resources and view the configuration of each. Notifications should be triggered each time a configuration changes, and Agencies should be given the ability to dig into the configuration history to perform incident analysis.

h. Monitoring of cloud resources with alerts to customers on security configuration gaps such as overly permissive access to certain compute instance ports and storage buckets, minimal use of role segregation using identity and access management (IAM), and weak password policies.

i. Automated security assessment service that helps improve the security and compliance of applications deployed on cloud by automatically assessing applications for vulnerabilities or

deviations from best practices. After performing an assessment, the tools should produce a detailed list of security findings prioritized by level of severity.

5.10. Exit Management / Transition-Out Responsibilities

a. Continuity and performance of the Services at all times including the duration of the Agreement and post expiry of the Agreement is a critical requirement of DIT, Manipur.

b. It is the prime responsibility of CSP to ensure continuity of service at all times of the Agreement including exit management period and in no way any facility/service shall be affected/degraded.

c. The responsibilities of Service Provider with respect to Exit Management/Transition-Out services on cloud include:

i. Provide necessary handholding and transition support to ensure the continuity and performance of the Services to the complete satisfaction of DIT, Manipur.

ii. Support DIT, Manipur in migration of the VMs, data, content and any other assets to the new environment created by DIT, Manipur or any Agency (on behalf of DIT, Manipur) on alternate cloud service provider's offerings to enable successful deployment and running of the DIT, Manipur's solution on the new infrastructure by providing a mechanism to DIT, Manipur for the bulk retrieval of all data, scripts, software, virtual machine images, and so forth to enable mirroring or copying to DIT, Manipur supplied industry standard media.

iii. The format of the data transmitted from the cloud service provider to DIT, Manipur should leverage standard data formats (e.g., OVF, VHD…) whenever possible to ease and enhance portability. The format will be finalized by DIT, Manipur.

iv. The ownership of the data generated upon usage of the system, at any point of time during the contract or expiry or termination of the contract, shall rest absolutely with DIT, Manipur.

v. Ensure that all the documentation required by DIT, Manipur for smooth transition including configuration documents are kept up to date and all such documentation is handed over to DIT, MANIPUR during regular intervals as well as during the exit management process. 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 DIT, Manipur.

vi. Once the exit process is completed, remove the DIT, Manipur 's data, content and other assets from the cloud environment and certify that the VM, Content and data destruction to DIT, Manipur as per stipulations and shall ensure that the data cannot be forensically recovered.

d. There shall not be any additional cost associated with the Exit / Transition-out process.

5.11. Service Level Agreement (SLA)

5.11.1. Measurement and Monitoring

a. The SLA parameters shall be monitored on monthly basis as per the individual SLA parameter requirements. However, if the performance of the system/services is degraded significantly at any given point in time during the contract and if the immediate measures are not implemented and issues are not rectified to the complete satisfaction of DIT, MANIPUR or an

agency designated by them, then DIT, MANIPUR will have the right to take services form another CSP at the cost of existing CSP or/and termination of the contract.

b. The full set of service level reports should be available to DIT, MANIPUR on a monthly basis or based on the project requirements.

c. The Monitoring Tools shall play a critical role in monitoring the SLA compliance and hence will have to be customized accordingly. The CSP shall make available the Monitoring tools for measuring and monitoring the SLAs. The bidder may deploy additional tools and develop additional scripts (if required) for capturing the required data for SLA report generation in automated way. The tools should generate the SLA Monitoring report in the end of every month which is to be shared with the DIT, Manipur on a monthly basis. DIT, Manipur or its nominated agency shall have full access to the Monitoring Tools/portal(and any other tools/solutions deployed for SLA measurement and monitoring) to extract data(raw, intermediate as well as reports) as required during the project. DIT, Manipur or its nominated agency will also audit the tool and the scripts on a regular basis.

d. The measurement methodology/criteria/logic will be reviewed by DIT, Manipur.

e. In case of default on any of the service level metric, the CSPs hall submit performance improvement plan along with the root cause analysis for DIT, Manipur's approval.

5.11.2. Periodic Reviews

a. During the contract period, it is envisaged that the recould be changes to the SLA, in terms of measurement methodology/logic/criteria, addition, alteration or deletion of certain parameters, based on mutual consent of both the parties, i.e. DIT, Manipur and CSP.

b. DIT, Manipur and CSP shall each ensure that the range of the Services under the SLA shall not be varied, reduced or increased except by the prior written agreement of DIT, MANIPUR and CSP in accordance with the Change Control Schedule.

c. The SLAs may be reviewed on an annual basis by DIT, Manipur in consultation with the CSP and other agencies.

5.11.3. Penalties

Payments to the CSP to be linked to the compliance with the SLA metrics laid down in the agreement.

a. The payment will be linked to the compliance with the SLA metrics.

b. The penalty in percentage of the monthly Payment is indicated against each SLA parameter in the table.

c. In case multiple SLA violations occur due to the same root cause or incident then the SLA that incurs the maximum penalty may be considered for penalty calculation rather than a sum of penalties for the applicable SLA violations.

d. Penalties shall not exceed 100% of the monthly bill.

e. If the penalties exceed more than 50% of the total monthly bill, it will result in a material breach .In case of a material breach, the operator will be given a cure period of one month to rectify the breach failing which a notice to terminate may be issued by DIT, Manipur.

5.12. Service Levels

S. No.	Service Level Objective	Measurement Methodology /	Target/Service Level	Penalty (Indicative)
Availability/Uptime				
1.	Availability/Uptime of cloud services Resources for Production environment (VMs, Storage, OS, VLB, Security Components,)	Availability (as per the definition in the SLA) will be measured for each of the underlying components (e.g., VM, Storage, OS, VLB, Security Components) provisioned in the cloud. Measured with the help of SLA reports provided by CSP.	Availability for each of the provisioned resources: >=99.5%	Default on any one or more of the provisioned resource will attract penalty as indicated below. <99.5% &>=99% (10% of the<<periodic Payment>>) < 99% (30% of the <<periodic Payment>>)
2.	Availability of Critical Services (e.g., Register Support Request or Incident; Provisioning/De-Provisioning; User Activation/De-Activation; User Profile Management; Access Utilization Monitoring Reports) over User/Admin Portal and APIs (where applicable) over User / Admin Portal and APIs (where applicable)	Availability (as per the definition in the SLA) will be measured for each of the critical services over both the User / Admin Portal and APIs (where applicable)	Availability for each of the critical services over both the User / Admin Portal and APIs (where applicable) >= 99.5%	Default on any one or more of the services on either of the portal or APIs will attract penalty as indicated below. <99.5% and >= 99% (10% of the<<Periodic Payment>>) <99% (20% of the <<Periodic Payment>>)
3.	Availability of Regular Reports (e.g., Audit, Certifications,) indicating the compliance to the Provisional Empanelment Requirements.		15 working days from the end of the quarter. If STQC issues a certificate	5% of <<periodic Payment>>
Support Channels – Incident and Helpdesk				
4.	Response Time	Average Time taken to acknowledge and respond, once a ticket/incident is logged through one of the agreed channels. This is calculated for all tickets/incidents reported within the reporting month.	95% within 15minutes	<95% &>=90% (5% of the <<periodic Payment>>) < 90% &>= 85% (7% of the<<periodic Payment>>) < 85% &>= 80% (9% of the<<periodic Payment>>)

5.	Time to Resolve - Severity 1	Time taken to resolve the reported ticket/incident from the time of logging.	For Severity 1, 98% of the incidents should be resolved within 30 minutes of problem reporting.	<98% &>=90% (5%of the <<periodic Payment>>) < 90% &>= 85% (10% of the<<periodic Payment>>) < 85% &>= 80% (20% of the<<periodic Payment>>)
7.	Time to Resolve -Severity 2,3	Time taken to resolve the reported ticket/incident from the time of logging.	95% of Severity 2 within 4 hours of problem reporting AND 95% of Severity 3 within 16 hours of problem reporting.	<95%&>=90% (2% of the <<periodic Payment>>) <90%&>=85% (4% of the <<periodic Payment>>) <85% &>= 80% (6% of the<<periodic Payment>>)
Vulnerability Management				
8.	Percentage of timely incident report	Measured as a percentage by the number of defined incidents reported within a predefined time(1 hour) limit after discovery, over the total number of defined incidents to the cloud service which are reported within a predefined period(i.e. month). Incident Response -CSP shall assess and acknowledge the defined incidents within 1 hour after discovery.	95% within 1 hour	<95%&>=90% (5% ofthe <<Periodic Payment>>) <90% &>= 85% (10% of the<<Periodic Payment>>) <85% &>= 80% (15% of the<<Periodic Payment>>)
9.	Percentage of timely incident resolutions	Measured as aPercentage of defined incidents against the cloud service that are resolved within a predefined time limit (month) over the total number of defined incidents to the cloud service within a predefined period. (Month). Measured from Incident Reports	95% to be resolved within 1 hour	<95%&>=90% (5% of the <<Periodic Payment>>) <90% &>= 85% (10%of the<<Periodic Payment>>) <85% &>= 80% (15% of the <<Periodic Payment>>)

Vulnerability Management				
10.	Percentage of timely vulnerability corrections	The number of vulnerability corrections performed by the cloud service provider- Measured as a percentage by the number of vulnerability corrections performed within a predefined time limit, over the total number of vulnerability corrections to the cloud service which are reported within a predefined period (i.e. month, week, year, etc.). • High Severity Vulnerabilities–30days - Maintain 99.95% service level • Medium Severity Vulnerabilities–90days - Maintain 99.95% Service level	99.95%	>=99% to <99.95% (10% the <<Periodic Payment>>) >=98%to<99% (20% ofthe <<Periodic Payment>>) <98% (30% of the <<Periodic Payment>>)
11.	Percentage of timely vulnerability reports	Measured as a percentage by the number of vulnerability reports within a predefined time limit, over the total number of vulnerability reports to the cloud service which are reported within a predefined period (i.e. month, week, year, etc.).	99.95%	>=99% to <99.95% (10% of the<<Periodic Payment>>) >=98%to<99% (20% of the<<Periodic Payment>>) <98% (30% of the<<Periodic Payment>>)
12.	Security breach including Data Theft/Loss/Corruption	Any incident wherein system compromised or any case where in data theft occurs(including internal incidents)	No breach	For each breach/data theft, penalty will be levied as per following criteria. Any security incident detected INR<<5Lakhs>>.This Penalty is applicable per incident. These penalties will not be part of overall SLA penalties cap per month. In case of serious breach of security wherein the data is stolen or corrupted, DIT, Manipur reserves the right to terminate the contract.

13.	Availability of SLA reports covering all parameters required for SLA monitoring within the defined time		(e.g.,3working days from the end of the month)	5% of <<periodic Payment>>

5.13. Severity Levels:

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

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

5.14. Definitions

i. **Cloud"ServiceLevelObjective"(SLO)**meansthetargetforagivenattributeofa cloud service that can be expressed quantitatively or qualitatively.

ii. **Cloud SLAs** means documented agreement between the cloud service provider and the Department that identifies services and cloud service level objectives (SLOs).

3. **Response time** is the time interval between a cloud service customer initiated event (e.g., logging of the request) and a cloud service provider initiated event in response to that stimulus.

iv. "**Scheduled Maintenance Time"** shall mean the time that the System is not in service due to a scheduled activity. Scheduled maintenance time is planned down time with the prior permission of the Department, during non-business hours.

The Scheduled Maintenance time<<within10hoursamonth>>as agreed shall not be considered for SLA Calculation.

v. "**Scheduled operation time**" means the scheduled operating hours of the System for the month. All scheduled maintenance time on the system would be deducted from the total operation time for the month to give the scheduled operation time.

i. **Availability" means** the time for which the cloud services and facilities are available for conducting operations on the Department system. Availability is defined as:

{(Scheduled Operation Time–System Downtime)/(Scheduled Operation Time)} *100%

vii. "**Incident**" refers to any event/issue that affects the normal functioning of the services/infrastructure, reported by the cloud consumer to the Cloud Service provider (CSP) can be termed as an Incident.

6. Bidding Terms and Conditions:

6.1. Evaluation of Bids:

a. Bids will be evaluated on the Basis of **Quality and Cost Based Selection (QCBS)** in the ratio of **70:30** for Technical and Financial Bids respectively.

b. The Bidding process shall be a two-stage process. Prior to the detailed evaluation of the Technical Bids, DIT shall determine whether each bid is (a) complete (b) is accompanied by the required information and documents and (c) is substantially responsive to the requirements set forth in the tender document. A substantially responsive Bid is one, which conforms to the requirements, terms, conditions and specifications of the Tender without any deviation .DIT's evaluation in this regard shall be final and binding on all Bidders.

c. Based on the results of the Technical evaluation and Technical presentation, DIT shall then proceed to open and evaluate the Commercial Bid of those Bidders who qualify in the Technical evaluation. The Commercial evaluation will take into account the information supplied by the Bidders in the Commercial Bid, and the same shall be evaluated in accordance with the evaluation criteria specified in the tender document.

d. DIT may at its sole discretion, waive any minor informality or non-conformity or irregularity in a Bid Document, which does not constitute a material deviation, provided such a waiver does not prejudice or affect the relative ranking of any Bidder

e. Secretary (IT), Government of Manipur will constitute the Tender Evaluation Committee. This committee will evaluate the Bid Documents submitted by the Bidders.

f. The Tender Evaluation Committee may choose to conduct technical negotiation or discussion with any or all the Bidders. The decision of the Evaluation Committee in the evaluation of the Technical and Commercial bids shall be final and binding on all the parties.

g. Any effort by a Bidder to influence the Tender Evaluation Committee's processing of Bids or award decisions may result in the rejection of the Bid.

6.2. Calculation of Bid:

a. The bidder with highest technical evaluation marks will be awarded 100% score. Technical score for other bidders will be evaluated using the following formula:

Tn= {(Technical Evaluation Marks of Bidder/Highest Technical Evaluation Marks) X 100} of 70%.

If three bidders A, B and C have Scored the following marks in the Technical bid:

a) A has scored of 40 marks.
b) B has scored of 50 marks.
c) C has scored of 60 marks.

Highest Technical Evaluation Marks is 60 marks and calculation for Technical Bid will be

For Bidder A TnA= (40/60 *100) of 70%
= 66.7 of 70/100
= 46.69
For Bidder B TnB= (50/60 *100) of 70%
= 83.3 of 70/100
= 58.31
For Bidder C TnC= (60/60 *100) of 30%
= 100 of 70/100
= 70

b. The bidder with lowest qualifying financial bid (L1) will be awarded 100% score. Financial score for other bidders will be evaluated using the following formula:

Fn= {(Financial Bid of L1/Financial Bid of Bidder)X 100} of 30%.

If three bidders A, B and C have submitted for financial bids in the following bid values:

a) A has submitted with bid value of Rs. 40.
b) B has submitted with bid value of Rs. 50.
c) C has submitted with bid value of Rs. 60.

Lowest qualifying financial bid (L1) will be Rs. 40 and calculation for Financial Bid will be

For Bidder A FnA= (40/40 *100) of 30%
= 100 of 30/100
= 30
For Bidder B FnB= (40/50 *100) of 30%
= 80 of 30/100
= 24
For Bidder C FnC= (40/60 *100) of 30%
= 66.7 of 30/100
= 20

c. The technical and financial scores secured by each bidder will be added using weightages of 70% and 30% respectively to compute Composite Score. The composite score will be computed as under:

BnA = (FnA+ TnA) =30+46.69=76 .69 marks.

BnB = (FnB+ TnB) = 24+58.31=82.31 marks

BnC = (FnC+ TnC) = 20+70=90 marks.

d. The bidder securing highest Composite Score will be adjudicated as most responsive bidder for award of works.

6.3. Correction of Errors:

Bidders are advised to exercise adequate care in quoting the prices. No excuse for corrections in the quoted price will be entertained after the proposals are opened. Corrections, if any, should be initiated by the person signing the proposal form before submission, failing which the figures for such items may not be considered.

Arithmetic errors in proposals will be corrected as follows:

i. In case of discrepancy between the amounts mentioned in figures and in words, the amount in words shall prevail.
ii. In case of discrepancy between the cost quoted in the pricing summary sheet for a component and the total cost provided for the component in the detailed cost breakup sheet, the cost quoted in the pricing summary sheet for the component will be considered.
iii. In case of discrepancy between the total price given for a line item / component and the calculated total price (number of units multiplied by the cost per unit for that line item), the calculated total price will be considered.
iv. The amount stated in the proposal form, adjusted in accordance with the above procedure, shall be considered as binding, unless it causes the overall proposal price to rise, in which case the proposal price shall prevail.
v. If the bidder does not accept the correction of errors, its bid will be rejected and EMD shall be forfeited.

6.4. PERIOD OF VALIDITY OF BIDS

a. **Validity Period**
Bids shall remain valid for 60 days after the date of bid opening prescribed by DIT, Manipur holds the right to reject a bid valid for a period shorter than 60 days as non-responsive, without any correspondence.

b. **Extension of Period of Validity**
In exceptional circumstances, DIT may solicit the Bidder's consent to an extension of the period of validity. The request and the response thereto shall be made in writing. Extension of validity period by the Bidder shall be unconditional. A Bidder granted extension of validity will not be permitted to modify his technical or commercial bid.

6 . 5 . Earnest Money Deposit:

i. Each bid must be accompanied by Earnest Money Deposit (EMD) of Rs. 5,00,000/- (Rupees two lakhs only) in the form of Demand Draft/Bankers Cheque/Bank Guarantee of any Nationalized/Scheduled commercial Bank taken in the name of Director, Directorate of Information Technology & Communication payable at Imphal. Bids received without Earnest Money Deposit are liable to be rejected.

ii. The original copy of EMD should reach to this office address as mentioned in the Notification on or before the time of opening of bid. The original should be hosted / couriered

/ given person to the concerned authority of DIT, Manipur latest by the last date and time of the bid submission otherwise uploaded bid will be rejected.

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

iv. EMD shall be valid for a period of Forty-five (45) days beyond the final bid validity period.

v. EMD of all unsuccessful bidders would be refunded by DIT, Manipur within 30 days of the bidder being notified by DIT, Manipur as being unsuccessful and after received a written request from the unsuccessful bidder for refund of the same. EMD of the successful bidder would be returned upon submission of Security Deposit.

vi. No interest shall be payable by DIT, Manipur to the Bidder(s) on the EMD amount for the period of its currency.

vii. The bid without adequate EMD, as mentioned above, will be liable for rejection without providing any further opportunity to the bidder concerned.

viii. The bidder shall extend the validity of the EMD on request by DIT, Manipur.

ix. EMD may be forfeited:
   a. If a bidder withdraws its bid during the period of bid validity or any extension thereof agreed to by the bidder
   b. In case of a successful bidder, if the bidder fails to submit the PBG in accordance with terms and conditions
   c. If any of the bidders modify their bid during the validity period
   d. If the Proposal is varied or modified in a manner not acceptable to IBM after opening of Proposal during the validity period or any extension thereof
   e. If the Bidder tries to influence/jeopardize the bidding/evaluation process or submits any forged documents.

6.6. Security Deposit

The Bidder shall at its own expense, deposit with department, within 30 days of the notification of award (done through issuance of the Work Order/Letter of Acceptance), an unconditional and irrevocable Performance Bank Guarantee (PBG) from Nationalized/Scheduled Bank as per the format placed at Section 6.7. of this Bid Document, payable on demand, for the due performance and fulfilment of the contract by the Bidder as **Security Deposit**. This Performance Bank Guarantee will be for an amount equivalent to 10% of Annual Bid Value. All charges whatsoever such as premium, commission, etc. with respect to the PBG shall be borne by the Bidder.

The PBG would be valid for a period of 3 more months from the date of validity of the Contract. The PBG may be discharged/ returned by department upon being satisfied that there has been due performance of the obligations of the Bidder under the contract. However, no interest shall be payable on the PBG. In the event, Bidder being unable to service the contract for whatever reason, department would evoke the PBG. Notwithstanding and without prejudice to any rights whatsoever of department under the Contract in the matter, the proceeds of the PBG shall be payable to department as compensation for any loss resulting from the Bidder's failure to complete its obligations under the Contract. Department shall notify the Bidder in writing of the exercise of its right to receive such

compensation within 14 days, indicating the contractual obligation(s) for which the Bidder is in default.

Department shall also be entitled to make recoveries from the Bidder's bills, PBG, or from any other amount due to him, the equivalent value of any payment made to him due to inadvertence, error, collusion, misconstruction or misstatement.

6.7. Performance Bank Guarantee Format

(For a sum of 10% of the value of the contract)

Ref.No.:

Date :

Bank Guarantee No.:

To

The Director (IT),
Government of Manipur

THIS INDENTURE made this ---------- day of ---------20---- BETWEEN THE ----------BANK incorporated under the English / Indian Companies Acts and carrying on business in <Address> (hereinafter referred to as 'the bank' which expression shall be deemed to include its successors and assigns) of the first part ---------- inhabitants carrying on business at ---------- in <Address> under the style and name of Messers ---------- (hereinafter referred to as 'the contractors') of the second part Shri----------

The Department of Information Technology, Government of Manipur, 4th Floor, West Block, New Secretariat Imphal -795001 (hereinafter referred to as DIT, Manipur which expression shall be deemed, also to include his successor or successors for the time being in the said office of DIT, Manipur) of the third part and THE <ADDRESS><ADDRESS> (hereinafter referred to as '<<>>') of the fourth part WHEREAS the contractors indemnify and keep indemnified the Corporation against any loss or damage that may be caused to or suffered by the Corporation by reason of any breach by the contractors of any of the terms and conditions of the contract that will be entered subsequently (within 15 days) and/or in the performance thereof against Letter of Intent number ---------- dated ---------- for the project **"Selection of Managed Service Provider/Cloud Service Provider for providing Cloud services for hosting all the applications/websites presently hosted in the Manipur SDC**" of ---------- department having tender No. No. 15/29/2017-DIT

amount Rs.---------- and the terms of such tender / contract require that the contractors shall deposit with the Commissioner as earnest money and/ or the security a sum of Rs.---------- (Rupees----------) AND WHEREAS if and when any such tender is accepted by the Commissioner, the contract to be entered into in furtherance thereof by the contractors will provide that such deposit shall remain with and will be appropriated by the Commissioner towards the Security Deposit to be taken under the contract and be redeemable by the contractors, if they shall duly and faithfully carry out the terms and provisions of such contract and shall duly satisfy all claims properly chargeable against them thereunder AND WHEREAS the contractors are constituents of the Bank and in order to facilitate the keeping of the accounts of the contractors, the Bank with the consent and concurrence of the contractors has requested the Commissioner to accept the undertaking of the Bank hereinafter contained, in place of the contractors depositing with the Commissioner the said sum as earnest money and/or the security as aforesaid AND WHEREAS accordingly the Commissioner has agreed to accept such undertaking. NOW THIS AGREEMENT WITNESSES that in consideration of the premises, the Bank at the request of the contractors (hereby testified) UNDERTAKES WITH the Commissioner to pay to the Commissioner upon demand in writing, whenever required by him, from time to time, so to do, a sum not exceeding in the whole Rs.---------- (Rupees----------) under the terms of the said tender and/or the contract. The B.G. is valid upto ----------

---

We agree that the decision of the Corporation, whether any breach of any of the terms and conditions of the contract and/or in the performance thereof has been committed by the Bidder and the amount of loss or damage that has been caused or suffered by the Corporation shall be final and binding on us and the amount of the said loss or damage shall be paid by us forthwith on demand and without demur to the Corporation.

"Notwithstanding anything what has been state above, our liability under the above guarantee is restricted to Rs. ---------- only and guarantee shall remain in force upto----------unless the demand or claim under this guarantee is made on us in writing on or before----------all your right under the above guarantee shall be forfeited and we shall be released from all liabilities under the guarantee thereafter".

IN WITNESS WHEREOF

WITNESS (1) ----------

Name and ----------

Address ----------

WITNESS (2) ----------

Name and ---------- the duly constituted Attorney Manager

Address ----------

The Bank and the said Messrs ----------

---------- (Name of the bank)

WITNESS (1) ----------

Name and ----------

Address ----------

WITNESS (2) ---------- for Messrs ----------

Name and ---------- (Name of the contractor)

Address ----------

Have hereinto set their respective hands the day and year first above written.

The undertaking-cum-indemnity bond is binding upon us/our heirs, executers, administrators, and assigns and/or successors and assigns.

_____

Signature of Authorized Signatory: Proprietor/Partners/Directors/POA holder (with official seal)

Place :

Date :

Name :

Designation :

Address :

Telephone & Fax :

E-mail address :

6.8. Work Completion Timelines & Payment Terms :

SL	Parameter	Timelines	Payment
2.	Setup of Cloud Environment and Handover the Cloud Environment to DIT, Manipur from the date of Issue and Acceptance of Work Order.	2 weeks	NIL
3.	Migration of the application on the new Cloud environment from the date of Issue and Acceptance of Work Order.	6 weeks	NIL
4.	Operational Acceptance from the date of Issue and Acceptance of Work Order from the date of Issue and Acceptance of Work Order.	10 weeks	NIL
5.	Operation and Maintenance phase	Will start from the date of operational acceptance provided by DIT, Manipur	Quarterly Payment (QP) for a period of 3 years.

Disbursement of payment to the Bidder is based on completion of tasks indicated in the implementation plan; Operations and Maintenance support plan and final handing over of O&M to the third party on completion at the end of three years of the contractual period.

Notes:

i. **Payment shall be made in Quarterly Basis**.
ii. Payment shall be made in INR.
iii. Adherence to timelines is critical for the success of the project.
iv. No advance payment shall be made for any activity.
v. If the Bidder is liable for any penalty as per the SLA (refer to the related clause of this agreement), the same shall be adjusted from payments due to the Bidder.
vi. DIT, Manipur will release the payment within 30 days of submission of valid invoice subject to the condition that invoice and all supporting documents produced are in order and work is performed as per the scope of the project and meeting the SLA Criteria. DIT, Manipur shall be entitled to delay or withhold the payment of a disputed invoice or part of it delivered by Bidder, when DIT, Manipur disputes such invoice or part of it, provided that such dispute is bonafide.
vii. No payment made by DIT, Manipur herein shall be deemed to constitute acceptance by DIT, Manipur of the system or any service
viii. In case Go-Live is delayed, the corresponding operations and maintenance phase will start after the Go-Live has been completed.
ix. A Project Implementation Committee (PIC) will be constituted which will be responsible for monitor the performance of the Bidder and recommend for the

payment.

x. If the Bidder is liable for any penalty/liquidated damages as per the SLA, the same shall be adjusted from monthly payments due to the service provider.

xi. All payments shall be made for the corresponding to the goods or services actually delivered, installed, or operationally accepted, per the Contract Implementation Schedule, at unit prices and in the currencies specified in the Commercial Bids.

6.9. Implementation related timelines and penalties

SL.	Parameter	Target	Basis	Penalty
1	Setup of Cloud Environment and Handover the Cloud Environment to DIT, Manipur.	Within 2 weeks from the issuance and acceptance of work Order.	This will be calculated on basis of days of delay	a) Within two weeks - Nil b) For every 5 days of delay 5% of QP. c) Delay of 10 days - 10% of QP d) Beyond 15 days - 50% of QP. The Bidder would be required to provide proper justification for the delay. If DIT, Manipur feels that the justification provided by the Bidder is not credible, the contract may be terminated.
2	Migration of the application on the new Cloud environment	Within 4 weeks after provisioning the services as mentioned in SL.No.1	This will be calculated on basis of days of delay	a) Within 4 weeks - Nil b) For every 7 days of delay 5% of QP. c) Delay of 30 days - 10% of QP d) Beyond 45 days - 50% of QP. The Bidder would be required to provide proper justification for the delay. If DIT, Manipur feels that the justification provided by the Bidder is not credible, the contract may be terminated.

6.10. General Terms and Conditions:

a. All costs and expenses incurred by bidder in any way associated with the development, preparation and submission of responses, including but not limited to attendance at meetings, discussions,

demonstrations, etc. and providing any additional information required by DIT Manipur, will be borne entirely and exclusively by the bidder.

b. DIT, Manipur may reject any or all the responses received/cancel the entire process at any stage without assigning any reason whatsoever

c. After the issue of the work order, formal contract agreement will be signed between the successful bidder and the Department.

d. No binding legal relationship will exist between any of the bidder and DIT, Manipur until execution of a contractual agreement.

e. DIT shall reserve the right to verify the operation and performance of Project by the Bidder and the Bidder shall permit DIT to do so. The DIT will evaluate the information submitted by the Bidder with regard to Bidder's capacity. **The Bidder cannot subcontract the work at any stage without prior written approval from the DIT.**

f. Bids received with incomplete information / documents shall be rejected. Bids not adhering to Terms, Conditions, Specifications and other details as given in this document may be summarily rejected**.**

g. All deviations from the Terms, Conditions and other details of Tender Document should be separately and clearly submitted.

h. This tender document is not transferable.

i. Modification or Withdrawal of Offers is not permissible after its submission. To assist in the scrutiny, evaluation and comparison of offers, DIT may, at its discretion, ask some or all Bidders for clarification of their offer.

j. The request for such clarifications and the response will necessarily be in writing.