Bid Number/बोली क्रमांक (बिड संख्या): GEM/2023/B/425064
Dated/दिनांक : 30-11-202

Bid Document/ बिड दस्तावेज़

Bid Details/बिड विवरण	
Bid End Date/Time/बिड बंद होने की तारीख/समय	19-12-2023 15:00:00
Bid Opening Date/Time/बिड खुलने की तारीख/समय	19-12-2023 15:30:00
Bid Offer Validity (From End Date)/बिड पेशकश वैधता (बंद होने की तारीख से)	120 (Days)
Ministry/State Name/मंत्रालय/राज्य का नाम	Ministry Of Education
Department Name/विभाग का नाम	Department Of Higher Education
Organisation Name/संगठन का नाम	Indian Institute Of Management (iim)
Office Name/कार्यालय का नाम	173025
Item Category/मद केटेगरी	Custom Bid for Services - Cloud Services for IIM Sirmaur
Contract Period/अनुबंध अवधि	3 Year(s)
Minimum Average Annual Turnover of the bidder (For 3 Years)/बिडर का न्यूनतम औसत वार्षिक टर्नओवर (3 वर्षों का)	50 Lakh (s)
Years of Past Experience Required for same/similar service/उन्हीं/समान सेवाओं के लिए अपेक्षित विगत अनुभव के वर्ष	5 Year (s)
Past Experience of Similar Services required/इसी तरह की सेवाओं का पिछला आवश्यक अनुभव है	Yes
MSE Exemption for Years Of Experience/अनुभव के वर्षों से एमएसई छूट/ and Turnover/टर्नओवर के लिए एमएसई को छूट प्राप्त है	Yes
Startup Exemption for Years Of Experience/अनुभव के वर्षों से स्टार्टअप छूट/ and Turnover/ टर्नओवर के लिए स्टार्टअप को छूट प्राप्त है	Yes
Document required from seller/विक्रेता से मांगे गए दस्तावेज़	Experience Criteria,Bidder Turnover,Certificate (Requested in ATC),OEM Authorization Certificate,OEM Annual Turnover,Additional Doc 1 (Requested in ATC),Additional Doc 2 (Requested in ATC),Additional Doc 3 (Requested in ATC),Additional Doc 4 (Requested in ATC) *In case any bidder is seeking exemption from Experience / Turnover Criteria, the supporting documents to prove his eligibility for exemption must be uploaded for evaluation by the buyer

Bid Details/बिड विवरण	
Bid to RA enabled/बिड से रिवर्स नीलामी सक्रिय किया	No
Type of Bid/बिड का प्रकार	Two Packet Bid
Time allowed for Technical Clarifications during technical evaluation/तकनीकी मूल्यांकन के दौरान तकनीकी स्पष्टीकरण हेतु अनुमत समय	2 Days
Estimated Bid Value/अनुमानित बिड मूल्य	1800000
Evaluation Method/मूल्यांकन पद्धति	Total value wise evaluation

EMD Detail/ईएमडी विवरण

Advisory Bank/एडवाईजरी बैंक	ICICI
EMD Amount/ईएमडी राशि	40000

ePBG Detail/ईपीबीजी विवरण

Advisory Bank/एडवाइजरी बैंक	ICICI
ePBG Percentage(%)/ईपीबीजी प्रतिशत (%)	10.00
Duration of ePBG required (Months)/ईपीबीजी की अपेक्षित अवधि (महीने).	38

(a). EMD EXEMPTION: The bidder seeking EMD exemption, must submit the valid supporting document for the releva
category as per GeM GTC with the bid. Under MSE category, only manufacturers for goods and Service Providers for
Services are eligible for exemption from EMD. Traders are excluded from the purview of this Policy./जेम की शर्तों के अनुसा
ईएमडी छूट के इच्छुक बिडर को संबंधित केटेगरी के लिए बिड के साथ वैध समर्थित दस्तावेज़ प्रस्तुत करने है। एमएसई केटेगरी के अंतर्गत केवल वस्तुओं
लिए विनिर्माता तथा सेवाओं के लिए सेवा प्रदाता ईएमडी से छूट के पात्र हैं। व्यापारियों को इस नीति के दायरे से बाहर रखा गया है।

(b). EMD & Performance security should be in favour of Beneficiary, wherever it is applicable./ईएमडी और संपादन जमानत
राशि, जहां यह लागू होती है, लाभार्थी के पक्ष में होनी चाहिए।

Beneficiary/लाभार्थी :
Office Assistant
173025, Department of Higher Education, Indian Institute of Management (IIM), Ministry of Education
(Gurmeet Kaur)

Splitting/विभाजन

Bid splitting not applied/बोली विभाजन लागू नहीं किया गया.

MII Compliance/एमआईआई अनुपालन

MII Compliance/एमआईआई अनुपालन	Yes

MSE Purchase Preference/एमएसई खरीद वरीयता

MSE Purchase Preference/एमएसई खरीद वरीयता	Yes

1. If the bidder is a Micro or Small Enterprise as per latest definitions under MSME rules, the bidder shall be exempte from the requirement of "Bidder Turnover" criteria and "Experience Criteria" subject to meeting of quality and techn specifications. If the bidder is OEM of the offered products, it would be exempted from the "OEM Average Turnover" criteria also subject to meeting of quality and technical specifications. In case any bidder is seeking exemption from Turnover / Experience Criteria, the supporting documents to prove his eligibility for exemption must be uploaded for evaluation by the buyer.
2. If the bidder is a Startup, the bidder shall be exempted from the requirement of "Bidder Turnover" criteria and "Experience Criteria" subject to their meeting of quality and technical specifications. If the bidder is OEM of the offer products, it would be exempted from the "OEM Average Turnover" criteria also subject to meeting of quality and technical specifications. In case any bidder is seeking exemption from Turnover / Experience Criteria, the supporting documents to prove his eligibility for exemption must be uploaded for evaluation by the buyer.
3. The minimum average annual financial turnover of the bidder during the last three years, ending on 31st March o the previous financial year, should be as indicated above in the bid document. Documentary evidence in the form of certified Audited Balance Sheets of relevant periods or a certificate from the Chartered Accountant / Cost Accountan indicating the turnover details for the relevant period shall be uploaded with the bid. In case the date of constitution incorporation of the bidder is less than 3-year-old, the average turnover in respect of the completed financial years after the date of constitution shall be taken into account for this criteria.
4. Years of Past Experience required: The bidder must have experience for number of years as indicated above in bi document (ending month of March prior to the bid opening) of providing similar type of services to any Central / Stat Govt Organization / PSU / Public Listed Company. Copies of relevant contracts / orders to be uploaded along with bid in support of having provided services during each of the Financial year.
5. Purchase preference to Micro and Small Enterprises (MSEs): Purchase preference will be given to MSEs as defined Public Procurement Policy for Micro and Small Enterprises (MSEs) Order, 2012 dated 23.03.2012 issued by Ministry o Micro, Small and Medium Enterprises and its subsequent Orders/Notifications issued by concerned Ministry. If the bidder wants to avail the Purchase preference for services, the bidder must be the Service provider of the offered Service. Relevant documentary evidence in this regard shall be uploaded along with the bid in respect of the offered service. If L-1 is not an MSE and MSE Service Provider (s) has/have quoted price within L-1+ 15% of margin of purchase preference /price band defined in relevant policy, then 100% order quantity will be awarded to such MSE bidder subject to acceptance of L1 bid price. OM_No.1_4_2021_PPD_dated_18.05.2023 for compliance of Concurrent application of Public Procurement Policy for Micro and Small Enterprises Order, 2012 and Public Procurement (Preference to Make in India) Order, 2017.
6. Estimated Bid Value indicated above is being declared solely for the purpose of guidance on EMD amount and for determining the Eligibility Criteria related to Turn Over, Past Performance and Project / Past Experience etc. This has relevance or bearing on the price to be quoted by the bidders and is also not going to have any impact on bid participation. Also this is not going to be used as a criteria in determining reasonableness of quoted prices which would be determined by the buyer based on its own assessment of reasonableness and based on competitive prices received in Bid / RA process.
7. Past Experience of Similar Services: The bidder must have successfully executed/completed similar Services over the last three years i.e. the current financial year and the last three financial years(ending month of March prior to tl bid opening): -
1. Three similar completed services costing not less than the amount equal to 40% (forty percent) of the estimated cost; or
2. Two similar completed services costing not less than the amount equal to 50% (fifty percent) of the estimated cos or
3. One similar completed service costing not less than the amount equal to 80% (eighty percent) of the estimated cc

Additional Qualification/Data Required/अतिरिक्त योग्यता /आवश्यक डेटा

Pre Qualification Criteria (PQC) etc if any required:1701160807.pdf

Scope of Work:1701160813.pdf

Service Level Agreement (SLA):1701160824.pdf

Payment Terms:1701160829.pdf

Any other Documents As per Specific Requirement of Buyer -1:1701160854.pdf

GEM Availability Report (GAR):1701161087.pdf

Custom Bid For Services - Cloud Services For IIM Sirmaur (1)

Technical Specifications/तकनीकी विशिष्टियाँ

Specification	Values
Core	
Description /Nomenclature of Service Proposed for procurement using custom bid functionality	Cloud Services for IIM Sirmaur
Regulatory/ Statutory Compliance of Service	YES
Compliance of Service to SOW, STC, SLA etc	YES
Addon(s)/एडऑन	

Additional Specification Documents/अतिरिक्त विशिष्टि दस्तावेज़

Consignees/Reporting Officer/परेषिती/रिपोर्टिंग अधिकारी

S.No./क्र. सं.	Consignee Reporting/Officer/परेषिती/रिपोर्टिंग अधिकारी	Address/पता	The quantity of procurement "1" indicates Project based or Lumpsum based hiring.	Additional Requirement/अतिरिक्त आवश्यकता
1	Gurmeet Kaur	173025,IIM Sirmaur, Rampur Ghat Road, Paonta Sahib PAN No-AAAAI9266R GSTIN-02AAAAI9266R1Z5	1	N/A

Buyer Added Bid Specific Terms and Conditions/क्रेता द्वारा जोड़ी गई बिड की विशेष शर्तें

1. **Generic**

   OPTION CLAUSE: The buyer can increase or decrease the contract quantity or contract duration up to 25 percent at the time of issue of the contract. However, once the contract is issued, contract quantity or contra duration can only be increased up to 25 percent. Bidders are bound to accept the revised quantity or duratio

2. **Past Project Experience**

   Proof for Past Experience and Project Experience clause: For fulfilling the experience criteria any one c the following documents may be considered as valid proof for meeting the experience criteria:a. Contract cop along with Invoice(s) with self-certification by the bidder that service/supplies against the invoices have been executed.b. Execution certificate by client with contract value.c. Any other document in support of contract execution like Third Party Inspection release note, etc.Proof for Past Experience and Project Experience clause For fulfilling the experience criteria any one of the following documents may be considered as valid proof for

meeting the experience criteria:a. Contract copy along with Invoice(s) with self-certification by the bidder tha service/supplies against the invoices have been executed.b. Execution certificate by client with contract value.c. Any other document in support of contract execution like Third Party Inspection release note, etc.

3. **Certificates**

   Bidder's offer is liable to be rejected if they don't upload any of the certificates / documents sought in the Bid document, ATC and Corrigendum if any.

4. **Generic**

   Bidder financial standing: The bidder should not be under liquidation, court receivership or similar proceedings, should not be bankrupt. Bidder to upload undertaking to this effect with bid.

5. **Service & Support**

   Dedicated /toll Free Telephone No. for Service Support : BIDDER/OEM must have Dedicated/toll Free Telephone No. for Service Support.

6. **Service & Support**

   Escalation Matrix For Service Support : Bidder/OEM must provide Escalation Matrix of Telephone Numbers for Service Support.

7. **Generic**

   1. The Seller shall not assign the Contract in whole or part without obtaining the prior written consent of buye
   2. The Seller shall not sub-contract the Contract in whole or part to any entity without obtaining the prior written consent of buyer.
   3. The Seller shall, notwithstanding the consent and assignment/sub-contract, remain jointly and severally liable and responsible to buyer together with the assignee/ sub-contractor, for and in respect of the due performance of the Contract and the Sellers obligations there under.

8. **Forms of EMD and PBG**

   Successful Bidder can submit the Performance Security in the form of Fixed Deposit Receipt also (besides PBG which is allowed as per GeM GTC). FDR should be made out or pledged in the name of

   THE DIRECTOR IIM SIRMAUR
   A/C (Name of the Seller). The bank should certify on it that the deposit can be withdrawn only on the demand with the sanction of the pledgee. For release of Security Deposit, the FDR will be released in favour of bidder b the Buyer after making endorsement on the back of the FDR duly signed and stamped along with covering letter. Successful Bidder has to upload scanned copy of the FDR document in place of PBG and has to ensure delivery of hard copy of Original FDR to the Buyer within 15 days of award of contract.

9. **Forms of EMD and PBG**

   Successful Bidder can submit the Performance Security in the form of Payment online through RTGS / internet banking also (besides PBG which is allowed as per GeM GTC). On-line payment shall be in Beneficiary name

   INDIAN INSTITUTE OF MANAGEMENT SIRMAUR
   Account No.
   140701000266
   IFSC Code
   ICIC0001407
   Bank Name
   ICICI
   Branch address
   PAONTA SAHIB DISTRICT SIRMAUR H.P. 173025
   . Successful Bidder to indicate Contract number and name of Seller entity in the transaction details field at the time of on-line transfer. Bidder has to upload scanned copy / proof of the Online Payment Transfer in place of PBG within 15 days of award of contract.

10. **Buyer Added Bid Specific ATC**

Buyer Added text based ATC clauses

BUYER ADDED SCOPE OF WORK & TECHNICAL QUALIFICATION CRITERIA FOR CLOUD SERVICES

1. Scope of Work for Provisioning, Deployment and Operations of Cloud Services: -

The scope of work contained in this RFP includes all activities for provisioning, configuring th cloud and thereafter to operate, maintain and support the provisioned and configured cloud nvironment for the entire duration of the contract period, as defined in the paras of this RFP he Cloud Service Provider (CSP)/Managed Service Provider (MSP) will provide services nece ary to setup the cloud infrastructure for IIM SIRMAUR under Meity guidelines for VPC Cloud. he broad scope of work for the CSP/MSP shall include:

I. Cloud Service offerings of CSP should be certified by MeitY for compliance to the publis ed standards and guidelines.

II. The billing would be done based on the duration for which the resources are active i.e. M SIRMAUR only pay for the resources that are consumed. No charges would be levied by the CSP/MSP when the resources are inactive.

III. CSP/MSP shall configure the entire cloud infra as per the requirement of IIM SIRMAUR ar enable the IIM SIRMAUR website and application partner to deploy the application. Any ch llenge related to deployment / upgradation / modification of application in cloud will be su pported by CSP/MSP. CSP/MSP Shall operate and maintain the cloud infra 24x7 and resolv all incidents, problems defined in SLA.

IV. For all the cloud services being quoted, the CSP/MSP has to ensure that all software bei offered are genuine and comply with the licensing policy of the software OEM.

V. CSP/MSP Shall provide the cloud service offerings for a combination of the Deployment odels as Iaas, Paas, SaaS.

VI. The CSP/MSP would be responsible for provisioning of required IT infrastructure as IaaS, aas and SaaS as per IIM SIRMAUR website and application hosting requirements.

VII. The proposed landscape for the deployment of website and Application solution is:

a) Test and Development (T&D)

b) User Acceptance Test (UAT)

c) Staging

d) Production

e) Others if required

VIII. The above use cases for deployment are only indicative and IIM SIRMAUR may requisite oud services for other purposes as well, whenever needed.

IX. The above environments are to be deployed on the VPC Cloud.

X. Each of the environments mentioned above shall be logically isolated.

XI. The CSP/MSP is required to have IPv6 support.

XII. The CSP/MSP shall be responsible for provisioning and deployment of required compute nfrastructure virtual machines, cloud native managed services, storage, security compon nt, Backup etc. for hosting IIM SIRMAUR applications. The indicative IT infrastructure requ ements are mentioned in separate section.

XIII. The CSP/MSP shall be responsible for provisioning and deployment of adequate Internet Bandwidth, including termination devices, for end users to access IIM SIRMAUR applicatio

XIV. The CSP/MSP shall be responsible for provisioning and deployment of IPSEC connectivity

over Internet between cloud setup and website and Application service provider as well a IIM SIRMAUR Office to enable access to manage the cloud services. IPSEC at IIM SIRMAUR nd and at website and Application provider end will be provided.

XV. The CSP/MSP will be responsible for provisioning and deployment of requisite network i rastructure services such as virtual firewall, VPC, ACLs and Load Balancer to ensure acce ibility of the cloud services as per defined architecture.

XVI. The CSP/MSP shall configure DNS to provide access the URLs (Public and Private) as pe IM SIRMAUR requirements.

XVII. CSP/MSP is required to propose the cloud native architecture wherever applicable in the ropose solution. The propose solution shall be independent of any platform / OEM and it c n be migrated to any other platform without any customization.

XVIII. The CSP/MSP shall configure the role base access of all the users who need access on p duction, Staging, UAT and other environments. Complete access management of hosted ebsite and application and services should be role based and reports shall be available to IM SIRMAUR.

XIX. Admin access to cloud components should be secure and only be accessible from VPN.

XX. The CSP/MSP shall ensure that all access, audit, system and security, API gateway logs hould be stored for audit purpose. IIM SIRMAUR will take decision to finalize the archive policy.

XXI. CSP/MSP Shall deploy and configure security components as per solution defined by IIM IRMAUR.

XXII. CSP/MSP shall submit the HLD/LLD to IIM SIRMAUR before provisioning the IT setup on c ud and should submit the As-Is post implementation.

XXIII. The cloud service provisioned and deploy by the CSP/MSP shall be scalable and allow III SIRMAUR to add/reduce cloud resources on demand basis whenever required.

XXIV. The CSP/MSP shall provide a portal that allows automation of cloud recourse manageme t, tracking, and optimization advisory.

XXV. CSP/MSP ensure the UAT and Staging cloud should scale down whenever IIM SIRMAUR i not performing the testing.

XXVI. The solution needs to provide the ability for IIM SIRMAUR IT Administrators to access the loud environment to view the metering, billing, and services available on cloud.

XXVII. CSP/MSP Shall provision and configure the backups for the data of VMs as per the polic pproved by IIM SIRMAUR.

XXVIII. CSP/MSP Shall provide the portal access to log the tickets for incidents and problems for M SIRMAUR users and IIM SIRMAUR Website and application provider.

XXIX. CSP/MSP Shall assign technical manager to IIM SIRMAUR (IIM SIRMAUR's authorize appli tion provider) for critical Incidents to on board the technical team to fix the issue on prior as per defined SLA.

XXX. CSP/MSP Shall provide the cloud native tools to monitor the performance of IT setup inc ding the compute, memory, disk, IOs bandwidth, application parameters and provisioned ervices.

XXXI. CSP/MSP Shall configure five dashboard to monitor the performance of IIM SIRMAUR clo d Infrastructure, as per the requirements of IIM SIRMAUR.

XXXII. CSP/MSP shall also customize the dashboard as per IIM SIRMAUR requirements, from tir to time.

XXXIII. CSP/MSP shall submit all the configured policies of Anti- DDos, firewall, load balancer, W F and other security components to IIM SIRMAUR and update the document wherever pol

y changes.

XXXIV. CSP/MSP shall provision and deploy the cloud services jointly with IIM SIRMAUR admin t m in IIM SIRMAUR office and provide all access to IIM SIRMAUR team or authorized par er.

XXXV. CSP/MSP shall provide the support to IIM SIRMAUR authorized application partner to de oy the Website and application on provisioned cloud.

XXXVI. IIM SIRMAUR will align third party partner to perform the VA (vulnerabilities assessmen on application and infra which is deployed on cloud. CSP/MSP should provide the neces ry support to IIM SIRMAUR partner to perform the same.

2. Security and Statutory Requirements

A. The CSP services need to be certified / compliant to the following standards based on t e cloud requirements:

I. ISO 27001 - Cloud services should be certified for the latest version of the st dards.

II. ISO/IEC 27017:2015-Code of practice for information security controls based ISO/IEC 27002 for cloud services and Information technology.

III. ISO 27018 - Code of practice for protection of personally identifiable informat n (PII) in Virtual Public clouds.

B. The CSP/MSP shall comply or meet any security requirements applicable to CSPs publis ed (or to be published) by Ministry of Electronics Information and Technology (MeitY), Gove ment of India

or any standards body setup / recognized by Government of India from time to time and no ed to the CSPs by MeitY as a mandatory standard.

C. The CSP/MSP shall meet all the security requirements indicated in the IT Act 2000 the rms and conditions of the Empanelment of the Cloud Service Providers and shall comply to t e audit criteria defined by STQC.

D. The CSP/MSP shall comply with the requirements of proposed Data Protection Act.

E. All the IIM SIRMAUR's data, which stored in cloud, should remain in data centers hoste n India and it should not go outside India.

F. CSP/MSP shall propose cloud services available from India location only.

G. CSP/MSP shall ensure that whenever IIM SIRMAUR ask to delete any data from cloud t n data should be deleted in all forms.

H. CSP/MSP Shall have provision for the below security components to secure the environ ent

(1) DDos protection

(2) Next Generation Firewall with capabilities to identify signature based and beha our based anomalies

(3) Anti-virus and HIPS (for virtual Machine)

(4) Data Encryption at rest and in transit

(5) SSL off-load/ Data protection

(6) Web Application Firewall (WAF)
(7) Advanced SIEM and Security Reporting
(8) Network Zoning
(9) Others (If required)

3. Migration

a) Technologies are changing very fast and IIM SIRMAUR would be needed to upgrade th cloud service time to time. CSP/MSP Shall plan the migration (within the same cloud) on new technologies available on cloud and ensure the error free migration of running workloads, D abased and other components based on decision taken by the IIM SIRMAUR.

b) MSP/CSP Shall not charge any extra amount other than charges applicable to new services. MSP/CSP Shall submit the plan for migration after discussion with IIM SIRMAUR and hird party application vendor authorize by IIM SIRMAUR.

c) Provisioning of new services and migration of existing services would be responsibilit f CSP/MSP. CSP/MSP would ensure the business downtime should be minimum.

4. Project Management and Governance

The CSP/MSP shall provide the details the governance framework in its proposal and can propos its own governance structure as part of response to this RFP. The CSP/MSP's proposed governa e model would be discussed between MSP and IIM SIRMAUR at the time of on boarding. The fin governance model shall be approved by IIM SIRMAUR.

CSP/MSP Shall appoint one Project Manager and he/she would meet formally on a monthly basi overing, at a minimum, the following agenda items:

a) Project Progress
b) Incidents and Problems report
c) Issues and concerns
d) Performance and SLA compliance reports
e) Unresolved and escalated issues
f) Change Management - Proposed changes, if any
g) Project risks and their proposed mitigation plan
h) Discussion on submitted deliverable
i) Timelines and anticipated delay in deliverable if any
j) Delays, if any – Reasons thereof and ways to make-up lost time
k) Any other issues that either party wishes to add to the agenda.

5. Project Monitoring and Reporting

CSP/MSP Shall submit the below defined reports by the first week of every month so that these r orts can be discussed on monthly review meeting. These reports are indicative and IIM SIRMAUR ay add more report as per requirements in operation phase.

CSP/MSP and IIM SIRMAUR mutually will form a steering committee that will monitor the progre of the project during implementation and in operation stage. This committee will meet a periodi nterval to ensure smooth functioning of the project

a) Incidents reported on monthly basis.

b) Incident resolution timelines with dates.
c) List of all VMs and their CPU performance average, Min and Max.
d) List of all VMs and their Memory performance average, Min and Max.
e) List of all Security appliances and their performance.
f) Bandwidth performance of all links.
g) List of storage disks and their IO performance.
h) SLA report as defined in section “Service level Agreement”.
i) List of changes planned, Change approved and implementation.
j) Performance of Databases
k) Performance of Cabernets containers
l) Performance of Security components

m) Security solution/SIEM Reports

n) DDos Reports

o) Others if required

6. Service Level Agreement

The key service level objectives that relate to the cloud services and the related aspects are in cated below:

a) The SLA parameters shall be monitored on a monthly basis as per the individual SLA p rameter requirements. However, if the performance of the system/services is degraded sign cantly at any given point in time during the contract and if the immediate measures are not mplemented and issues are not rectified to the complete satisfaction of IIM SIRMAUR, then e Client will have the right to take appropriate disciplinary actions including termination of t e contract.
b) The full set of service level reports should be available to the IIM SIRMAUR on a month basis or based on the project requirements.
c) The Monitoring Tools shall play a critical role in monitoring the SLA compliance and he ce will have to be customized accordingly. The CSP/MSP shall make available the Monitoring ools for measuring and monitoring the SLAs. The CSP/MSP may deploy additional tools and d velop additional scripts (if required) for capturing the required data for SLA report generati in automated way. The tools should generate the SLA Monitoring report in the end of every month which is to be shared with the IIM SIRMAUR on a monthly basis. IIM SIRMAUR sha have full access to the Monitoring Tools/portal and any other tools / solutions deployed for S A measurement and monitoring) to extract data as required during the project.
d) The measurement methodology / criteria / logic will be reviewed by IIM SIRMAUR.
e) In case of default on any of the service level metric, the CSP/MSP shall submit perfor nce improvement plan along with the root cause analysis for the IIM SIRMAUR approval.
f) In case these service levels cannot be achieved at service levels defined in the agree ment, IIM SIRMAUR shall invoke the performance related penalties. Payments to the Supplie will be linked to the compliance with the SLA metrics laid down in the agreement.

S No	Service Level Objective	Measurement Methodology	Target	Penalty

1	Availability of all provisioned Services which are provided by CSP/ MSP including VM, Storage, DB, API gateways security services and any other critical services	Availability (as per the definition in the SLA) will be measured for each of the services over both the public users and admin users irrespective of service of any data centre	Availability for each of the services over both the User / Admin Portal and APIs (where applicable) >= 99.99%	Default on any one or more of the services will attract penalty as indicated below. <99.99% and >= 99.5% (3% of the Periodic Payment) <99.5% (5% of the Periodic Payment)
2	Availability of the links Internet and MPLS	Availability (as per the definition in the SLA) will be measured for each of the network links provisioned in the cloud to access the portal or admin services	Availability for each of the links: >= 99.99%	Default on any one or more of the provisioned links will attract penalty as indicated below. <99.99% & >=99.5% (3% of the periodic Payment) < 99.5% (5% of the periodic Payment)
3	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 15 minutes	<95% & >=90% (3% of the periodic Payment) < 90 (5% of the periodic Payment)
4	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 Shall be resolved within 2 Hours of the reporting	<98% & >=90% (3% of the periodic Payment) < 90% (5% of the periodic Payment)
5	Time to Resolve - Severity 2	Time taken to resolve the reported ticket/incident from the time of logging.	95% of Severity 2 within 6 hours of Incident reporting	<95% & >=90% (3% of the periodic Payment) < 90% & (5% of the periodic Payment)
6	Security breach including Data Theft/Loss/ Corruption/ unauthorized access	Any incident where in system compromised or any case wherein data theft occurs (including internal incidents)	No breach	Any security incident detected than penalty will be INR 5 Lakhs for each incident. This penalty is applicable per incident.

7	Availability of SLA reports covering all parameters required for SLA monitoring within the defined time	10 working days from the end of the month	10 working days from the end of the month	5% of periodic Payment
8	Availability of Root Cause Analysis (RCA) ports for Severity 1 & 2		Average within 10 Working days	5% of periodic Payment
9	Setup of Cloud Environment	2 weeks from PO/LOA	No Delay	5% of one time implementation cost per week delay

Note:

- Periodic Payment means Monthly Payment.
- Days: All Working and Non-working days (365 days in a calendar year)
- 24*7 means three shifts of 8 hours every day. This is applicable for all seven days of the week without any non-working days.
- Severity Levels: Below severity definition, provide indicative scenarios for defining Incident severity. However, GSTN 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	Production Environment is down or critical malfunction resulting in an inoperative condition or disrupts critical business functions and requires immediate attention.	Non-availability of VM, Storage, API gateway, DB, Internet link and application containers and all security services.
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, The environment is usable but severely limited.	Intermittent network connectivity, UAT and SIT environment.

NOTE:

a) **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.

b) **Scheduled Maintenance** time shall mean the time that the System is not in service due t

scheduled activity. Scheduled maintenance time is planned downtime with the prior permission o he Department, during non-business hours. The Scheduled Maintenance time, within 10 hours a n nth shall not be considered for SLA Calculation.

c) **Scheduled operation time** means the scheduled operating hours of the System for the m th. All scheduled maintenance time on the system would be deducted from the total operation tir for the month to give the scheduled operation time.

d) **Availability means** the time for which the cloud services and facilities are available for co ucting operations for the IIM SIRMAUR application running on cloud. Availability is defined as: {(Sc eduled Operation Time – System Downtime) / (Scheduled Operation Time)} * 100%

e) **Incident** refers to any event/issue that affects the normal functioning of the services / infra ructure, reported by the IIM SIRMAUR or Users who are using application hosted on the Cloud Ser ce provider (CSP) can be termed as an Incident.

Qualification Criteria

–

Qualification for Cloud Service Provider (CSP)

#	CSP Mandatory Criteria	Documentary Evidence
1	The Cloud Service Provider (CSP) should have been o ffering services in India from at least last 3 financial y ears with average annual turnover of at least Rs. 50 Lakh.	Copy of Certificate of Incorporation or C ertified copy of Partnership Deed Letter from Statutory Auditors / Certific ate from Chartered Accountant on their letterhead mentioning the annual reven ue in India
2	The Cloud Service Provider (CSP) should be empanel ed with the Ministry of Electronics & Information and Technology (MEITY), Government of India for offering both DC & DR on its own to government bodies. The CSP Data centers offered for services shall be locate d in different seismic zone within India.	Undertaking on CSP letterhead confirmi ng the clause and copy of Valid MEITY E mpanelment Certificate
3	The CSP’s proposed DC & DR center should be operat ional and live for minimum last 2 years.	Undertaking on CSP letterhead confirmi ng the clause.

4	CSP shall have published on its public/Meity website - cloud services' rates for India, Service Level Agreements (SLAs), dashboard live-status of cloud services' health across global data centre and outage details (if any) with RCA.	An undertaking from the CSP with the links to its relevant public facing website (s) covering the details
5	The proposed Cloud should have Managed cloud native database services for Postgre SQL and My SQL enterprises	Undertaking on CSP letterhead with link to public facing website having the service and functionality description
6	CSP must have their security service in cloud for- • NextGen Firewall • Web Application Firewall • DDoS Protection • Data Encryption at rest • Identity and Access Management - fine grained access control for access to cloud resources: Only the resource with appropriate permissions and grants has access to any specific resource and All access and changes carried out are logged, cannot be tampered with and be auditable.	Undertaking on CSP letterhead with link to public facing website having the service and functionality description
7	Uptime offered on a single VM instance is equal or more than 99.5 %	Undertaking on CSP letterhead with link to public facing website having the service and functionality description
8	• Tier-3 datacenter certification from TIA or equivalent agency (Documentary Evidence-Certificate/) • ISO/IEC 27701:2019 Security techniques —ISO /IEC 27001 • ISO 27017 • ISO 27018 • ISO 9001 • ISO 22301 • PCI-DSS Complied • SOC 1/2/3 Certificate/audited Report • ISO 20000-1	Copy of Relevant Certificate
9	CSP should provide the capability to scale storage automatically without any manual intervention and downtime. This should help customers to pay only for the used capacity rather than unused allocated storage to VM.	Undertaking on CSP letterhead with link to public facing website having the service and functionality description

10	The proposed cloud should provide the latest generation processors with complete flexibility of compute shapes. Customers should have the option to choose any combination of CPU core and memory rather than fixed-sized shapes.	Undertaking on CSP letterhead with link to public facing website having the service and functionality description

Pre-qualification for Managed Service Provider (MSP)

–

Sl. No	Minimum Qualifications Criteria	Documentary proof to be submitted
1.	The Bidder should be – A company incorporated under the Indian Companies Act, 2013 or any other previous company law as per section 2 (20) of the Indian Companies Act 2013/ Partnerships Firm registered under the Limited Liability Partnerships or Partnership Act Registered with the GST Authorities Company should have a valid PAN number	Certificate of Incorporation; and GST Registration certificate issued by GSTN authorities (copy), PAN Card (copy).
2.	The Bidder should have an average annual turnover of at least INR 50 Lakh from IT/ITES services in last three financial years (i.e. FY 2020-21, FY 2021-22 and FY 2022-23).	Duly Audited Financial Statements by the CA/ statutory auditor certificate or certificate from Company Secretary of Bidder specifying the net worth for the specified year.
3.	Bidder (MSP) should have following certifications: • ISO9001, • ISO27001, • CMMI Level 3	Copy of certification
4.	Bidder should have executed at least two work order with value of INR 50 lakh each or more from PSU/Central Government /Corporate/Autonomous bodies or similar Institutes/organizations in last 5 financial years to provide Cloud Services.	Copy of Work Orders/Completion certificates duly signed & stamped by the issuing authority.
5.	Bidder has direct reseller authorization with proposed CSP.	Reseller Authorization Certificate from CSP
6.	Bidder has at least 10 technical certified resources (in active employment) for any CSP.	Undertaking from the HR / Copy of Certificate

7.	Submission of “Undertaking of Not Being blacklisted t hat, the firm or none of the firm’s Partners or Director s have been blacklisted in India by any Indian State / Central Governments Dept. / Public Sector Undertakin g of India during last 5 year.	Self-attested Undertaking
8.	Bidder to provide OEM authorization letter/ Manufactu rers Authorization Certificate from the MeitY Empanel ed OEM quoting this tender reference number, date	OEM Manufacturers Authorization Certificate h empanelment confirmation from MeitY

Other Terms & Conditions:

01. The period of services will be for a period of three years w.e.f. the date of implementation. The Compe nt authority of this Institute reserves the right to terminate the contract at any point of time by giving ne-month notice period.

02. If any dispute arises between the parties, the court for jurisdiction shall be at the Court of Paonta Sahi Himachal Pradesh only.

03. Payment will be released on the submission of the Original Invoices on monthly basis after TDS deduc ns as applicable.

.

11. **Buyer Added Bid Specific ATC**

    Buyer uploaded ATC document Click here to view the file.

12. **Buyer Added Bid Specific SLA**

    File Attachment Click here to view the file.

Disclaimer/अस्वीकरण

The additional terms and conditions have been incorporated by the Buyer after approval of the Competent Authority in Buyer Organization, whereby Buyer organization is solely responsible for the impact of these clauses on the biddi process, its outcome, and consequences thereof including any eccentricity / restriction arising in the bidding proces due to these ATCs and due to modification of technical specifications and / or terms and conditions governing the bi Any clause(s) incorporated by the Buyer regarding following shall be treated as null and void and would not be considered as part of bid:-

1. Definition of Class I and Class II suppliers in the bid not in line with the extant Order / Office Memorandum issued by DPIIT in this regard.
2. Seeking EMD submission from bidder(s), including via Additional Terms & Conditions, in contravention to exemption provided to such sellers under GeM GTC.
3. Publishing Custom / BOQ bids for items for which regular GeM categories are available without any Category item bunched with it.
4. Creating BoQ bid for single item.
5. Mentioning specific Brand or Make or Model or Manufacturer or Dealer name.

6. Mandating submission of documents in physical form as a pre-requisite to qualify bidders.
7. Floating / creation of work contracts as Custom Bids in Services.
8. Seeking sample with bid or approval of samples during bid evaluation process.
9. Mandating foreign / international certifications even in case of existence of Indian Standards without specifyir equivalent Indian Certification / standards.
10. Seeking experience from specific organization / department / institute only or from foreign / export experienc
11. Creating bid for items from irrelevant categories.
12. Incorporating any clause against the MSME policy and Preference to Make in India Policy.
13. Reference of conditions published on any external site or reference to external documents/clauses.
14. Asking for any Tender fee / Bid Participation fee / Auction fee in case of Bids / Forward Auction, as the case m be.

Further, if any seller has any objection/grievance against these additional clauses or otherwise on any aspect of this bid, they can raise their representation against the same by using the Representation window provided in the bid details field in Seller dashboard after logging in as a seller within 4 days of bid publication on GeM. Buyer is duty bound to reply to all such representations and would not be allowed to open bids if he fails to reply to such representations.

This Bid is governed by the General Terms and Conditions/सामान्य नियम और शर्तें, conditons stipulated in Bid and Service Level Agreement specific to this Service as provided in the Marketplace. However in case if any condition specified in General Terms and Conditions/सामान्य नियम और शर्तें is contradicted by the conditions stipulated in Service Level Agreement, then it will over ride the conditions in the General Terms and Conditions.

In terms of GeM GTC clause 26 regarding Restrictions on procurement from a bidder of a country which shares a land border with India, any bidder from a country which shar land border with India will be eligible to bid in this tender only if the bidder is registered with the Competent Authority. While participating in bid, Bidder has to undert compliance of this and any false declaration and non-compliance of this would be a ground for immediate termination of the contract and further legal action in accordance the laws./जेम की सामान्य शर्तों के खंड 26 के संदर्भ में भारत के साथ भूमि सीमा साझा करने वाले देश के बिडर से खरीद पर प्रतिबंध के संबंध भारत के साथ भूमि सीमा साझा करने वाले देश का कोई भी बिडर इस निविदा में बिड देने के लिए तभी पात्र होगा जब वह बिड देने वाला स प्राधिकारी के पास पंजीकृत हो।बिड में भाग लेते समय बिडर को इसका अनुपालन करना होगा और कोई भी गलत घोषणा किए जाने व इस अनुपालन न करने पर अनुबंध को तत्काल समाप्त करने और कानून के अनुसार आगे की कानूनी कार्रवाई का आधार होगा।

---Thank You/धन्यवाद---

BUYER ADDED SCOPE OF WORK & TECHNICAL QUALIFICATION CRITERIA FOR CLOUD SERVICES

1. Scope of Work for Provisioning, Deployment and Operations of Cloud Services: -

The scope of work contained in this RFP includes all activities for provisioning, configuring the cloud and thereafter to operate, maintain and support the provisioned and configured cloud environment for the entire duration of the contract period, as defined in the paras of this RFP. The Cloud Service Provider (CSP)/Managed Service Provider (MSP) will provide services necessary to setup the cloud infrastructure for IIM SIRMAUR under Meity guidelines for VPC Cloud. The broad scope of work for the CSP/MSP shall include:

I. Cloud Service offerings of CSP should be certified by MeitY for compliance to the published standards and guidelines.
II. The billing would be done based on the duration for which the resources are active i.e. IIM SIRMAUR only pay for the resources that are consumed. No charges would be levied by the CSP/MSP when the resources are inactive.
III. CSP/MSP shall configure the entire cloud infra as per the requirement of IIM SIRMAUR and enable the IIM SIRMAUR website and application partner to deploy the application. Any challenge related to deployment / upgradation / modification of application in cloud will be supported by CSP/MSP. CSP/MSP Shall operate and maintain the cloud infra 24x7 and resolve all incidents, problems defined in SLA.
IV. For all the cloud services being quoted, the CSP/MSP has to ensure that all software being offered are genuine and comply with the licensing policy of the software OEM.
V. CSP/MSP Shall provide the cloud service offerings for a combination of the Deployment Models as Iaas, Paas, SaaS.
VI. The CSP/MSP would be responsible for provisioning of required IT infrastructure as IaaS, Paas and SaaS as per IIM SIRMAUR website and application hosting requirements.
VII. The proposed landscape for the deployment of website and Application solution is:
    a) Test and Development (T&D)
    b) User Acceptance Test (UAT)
    c) Staging
    d) Production
    e) Others if required

VIII. The above use cases for deployment are only indicative and IIM SIRMAUR may requisite cloud services for other purposes as well, whenever needed.
IX. The above environments are to be deployed on the VPC Cloud.

X. Each of the environments mentioned above shall be logically isolated.

XI. The CSP/MSP is required to have IPv6 support.

XII. The CSP/MSP shall be responsible for provisioning and deployment of required compute infrastructure virtual machines, cloud native managed services, storage, security component, Backup etc. for hosting IIM SIRMAUR applications. The indicative IT infrastructure requirements are mentioned in separate section.

XIII. The CSP/MSP shall be responsible for provisioning and deployment of adequate Internet Bandwidth, including termination devices, for end users to access IIM SIRMAUR application.

XIV. The CSP/MSP shall be responsible for provisioning and deployment of IPSEC connectivity over Internet between cloud setup and website and Application service provider as well as IIM SIRMAUR Office to enable access to manage the cloud services. IPSEC at IIM SIRMAUR end and at website and Application provider end will be provided.

XV. The CSP/MSP will be responsible for provisioning and deployment of requisite network infrastructure services such as virtual firewall, VPC, ACLs and Load Balancer to ensure accessibility of the cloud services as per defined architecture.

XVI. The CSP/MSP shall configure DNS to provide access the URLs (Public and Private) as per IIM SIRMAUR requirements.

XVII. CSP/MSP is required to propose the cloud native architecture wherever applicable in the propose solution. The propose solution shall be independent of any platform / OEM and it can be migrated to any other platform without any customization.

XVIII. The CSP/MSP shall configure the role base access of all the users who need access on production, Staging, UAT and other environments. Complete access management of hosted website and application and services should be role based and reports shall be available to IIM SIRMAUR.

XIX. Admin access to cloud components should be secure and only be accessible from VPN.

XX. The CSP/MSP shall ensure that all access, audit, system and security, API gateway logs should be stored for audit purpose. IIM SIRMAUR will take decision to finalize the archive policy.

XXI. CSP/MSP Shall deploy and configure security components as per solution defined by IIM SIRMAUR.

XXII. CSP/MSP shall submit the HLD/LLD to IIM SIRMAUR before provisioning the IT setup on cloud and should submit the As-Is post implementation.

XXIII. The cloud service provisioned and deploy by the CSP/MSP shall be scalable and allow IIM SIRMAUR to add/reduce cloud resources on demand basis whenever required.

XXIV. The CSP/MSP shall provide a portal that allows automation of cloud recourse management, tracking, and optimization advisory.

XXV. CSP/MSP ensure the UAT and Staging cloud should scale down whenever IIM SIRMAUR is not performing the testing.

XXVI. The solution needs to provide the ability for IIM SIRMAUR IT Administrators to access the cloud environment to view the metering, billing, and services available on cloud.

XXVII. CSP/MSP Shall provision and configure the backups for the data of VMs as per the policy approved by IIM SIRMAUR.

XXVIII. CSP/MSP Shall provide the portal access to log the tickets for incidents and problems for IIM SIRMAUR users and IIM SIRMAUR Website and application provider.

XXIX. CSP/MSP Shall assign technical manager to IIM SIRMAUR (IIM SIRMAUR's authorize application provider) for critical Incidents to on board the technical team to fix the issue on priority as per defined SLA.

XXX. CSP/MSP Shall provide the cloud native tools to monitor the performance of IT setup including the compute, memory, disk, IOs bandwidth, application parameters and provisioned services.

XXXI. CSP/MSP Shall configure five dashboard to monitor the performance of IIM SIRMAUR cloud Infrastructure, as per the requirements of IIM SIRMAUR.

XXXII. CSP/MSP shall also customize the dashboard as per IIM SIRMAUR requirements, from time to time.

XXXIII. CSP/MSP shall submit all the configured policies of Anti- DDos, firewall, load balancer, WAF and other security components to IIM SIRMAUR and update the document wherever policy changes.

XXXIV. CSP/MSP shall provision and deploy the cloud services jointly with IIM SIRMAUR admin team in IIM SIRMAUR office and provide all access to IIM SIRMAUR team or authorized partner.

XXXV. CSP/MSP shall provide the support to IIM SIRMAUR authorized application partner to deploy the Website and application on provisioned cloud.

XXXVI. IIM SIRMAUR will align third party partner to perform the VA (vulnerabilities assessment) on application and infra which is deployed on cloud. CSP/MSP should provide the necessary support to IIM SIRMAUR partner to perform the same.

2. Security and Statutory Requirements

A. The CSP services need to be certified / compliant to the following standards based on the cloud requirements:

   I. ISO 27001 - 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 Virtual Public clouds.

B. The CSP/MSP shall comply or meet any security requirements applicable to CSPs 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 CSPs by MeitY as a mandatory standard.

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

D. The CSP/MSP shall comply with the requirements of proposed Data Protection Act.

E. All the IIM SIRMAUR's data, which stored in cloud, should remain in datacenters hosted in India and it should not go outside India.

F. CSP/MSP shall propose cloud services available from India location only.

G. CSP/MSP shall ensure that whenever IIM SIRMAUR ask to delete any data from cloud than data should be deleted in all forms.

H. CSP/MSP Shall have provision for the below security components to secure the environment

(1) DDos protection
(2) Next Generation Firewall with capabilities to identify signature based and behaviour based anomalies
(3) Anti-virus and HIPS (for virtual Machine)
(4) Data Encryption at rest and in transit
(5) SSL off-load/ Data protection
(6) Web Application Firewall (WAF)
(7) Advanced SIEM and Security Reporting
(8) Network Zoning
(9) Others (If required)

3. Migration

a) Technologies are changing very fast and IIM SIRMAUR would be needed to upgrade the cloud service time to time. CSP/MSP Shall plan the migration (within the same cloud) on new technologies available on cloud and ensure the error free migration of running workloads, Databased and other components based on decision taken by the IIM SIRMAUR.

b) MSP/CSP Shall not charge any extra amount other than charges applicable to new services. MSP/CSP Shall submit the plan for migration after discussion with IIM SIRMAUR and third party application vendor authorize by IIM SIRMAUR.

c) Provisioning of new services and migration of existing services would be responsibility of CSP/MSP. CSP/MSP would ensure the business downtime should be minimum.

4. Project Management and Governance

The CSP/MSP shall provide the details the governance framework in its proposal and can propose its own governance structure as part of response to this RFP. The CSP/MSP's proposed governance model would be discussed between MSP and IIM SIRMAUR at the time of on boarding. The final governance model shall be approved by IIM SIRMAUR.

CSP/MSP Shall appoint one Project Manager and he/she would meet formally on a monthly basis covering, at a minimum, the following agenda items:

a) Project Progress
b) Incidents and Problems report
c) Issues and concerns
d) Performance and SLA compliance reports
e) Unresolved and escalated issues
f) Change Management - Proposed changes, if any
g) Project risks and their proposed mitigation plan
h) Discussion on submitted deliverable
i) Timelines and anticipated delay in deliverable if any
j) Delays, if any – Reasons thereof and ways to make-up lost time
k) Any other issues that either party wishes to add to the agenda.

5. Project Monitoring and Reporting

CSP/MSP Shall submit the below defined reports by the first week of every month so that these reports can be discussed on monthly review meeting. These reports are indicative and IIM SIRMAUR may add more report as per requirements in operation phase.

CSP/MSP and IIM SIRMAUR mutually will form a steering committee that will monitor the progress of the project during implementation and in operation stage. This committee will meet a periodic interval to ensure smooth functioning of the project

a) Incidents reported on monthly basis.
b) Incident resolution timelines with dates.
c) List of all VMs and their CPU performance average, Min and Max.
d) List of all VMs and their Memory performance average, Min and Max.
e) List of all Security appliances and their performance.
f) Bandwidth performance of all links.
g) List of storage disks and their IO performance.
h) SLA report as defined in section "Service level Agreement".
i) List of changes planned, Change approved and implementation.
j) Performance of Databases
k) Performance of Cabernets containers
l) Performance of Security components

m) Security solution/SIEM Reports
n) DDos Reports
o) Others if required

6. Service Level Agreement

The key service level objectives that relate to the cloud services and the related aspects are indicated below:

a) The SLA parameters shall be monitored on a 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 IIM SIRMAUR, then the Client will have the right to take appropriate disciplinary actions including termination of the contract.
b) The full set of service level reports should be available to the IIM SIRMAUR 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/MSP shall make available the Monitoring tools for measuring and monitoring the SLAs. The CSP/MSP 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 IIM SIRMAUR on a monthly basis. IIM SIRMAUR shall have full access to the Monitoring Tools/portal and any other tools / solutions deployed for SLA measurement and monitoring) to extract data as required during the project.
d) The measurement methodology / criteria / logic will be reviewed by IIM SIRMAUR.
e) In case of default on any of the service level metric, the CSP/MSP shall submit performance improvement plan along with the root cause analysis for the IIM SIRMAUR approval.
f) In case these service levels cannot be achieved at service levels defined in the agreement, IIM SIRMAUR shall invoke the performance related penalties. Payments to the Supplier will be linked to the compliance with the SLA metrics laid down in the agreement.

S No	Service Level Objective	Measurement Methodology	Target	Penalty
1	Availability of all provisioned Services which are provided by CSP/MSP including VM, Storage, DB, API gateways security services and any other critical services	Availability (as per the definition in the SLA) will be measured for each of the services over both the public users and admin users irrespective of service of any data centre	Availability for each of the services over both the User / Admin Portal and APIs (where applicable) >= 99.99%	Default on any one or more of the services will attract penalty as indicated below. <99.99% and >= 99.5% (3% of the Periodic Payment) <99.5% (5% of the Periodic Payment)
2	Availability of the links Internet and MPLS	Availability (as per the definition in the SLA) will be measured for each of the network links provisioned in the cloud to access the portal or admin services	Availability for each of the links: >= 99.99%	Default on any one or more of the provisioned links will attract penalty as indicated below. <99.99% & >=99.5% (3% of the periodic Payment) < 99.5% (5% of the periodic Payment)
3	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 15 minutes	<95% & >=90% (3% of the periodic Payment) < 90 (5% of the periodic Payment)

4	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 Shall be resolved within 2 Hours of the reporting	<98% & >=90% (3% of the periodic Payment) < 90% (5% of the periodic Payment)
5	Time to Resolve - Severity 2	Time taken to resolve the reported ticket/incident from the time of logging.	95% of Severity 2 within 6 hours of Incident reporting	<95% & >=90% (3% of the periodic Payment) < 90% & (5% of the periodic Payment)
6	Security breach including Data Theft/Loss/ Corruption/ unauthorized access	Any incident where in system compromised or any case wherein data theft occurs (including internal incidents)	No breach	Any security incident detected than penalty will be INR 5 Lakhs for each incident. This penalty is applicable per incident.
7	Availability of SLA reports covering all parameters required for SLA monitoring within the defined time	10 working days from the end of the month	10 working days from the end of the month	5% of periodic Payment
8	Availability of Root Cause Analysis (RCA) ports for Severity 1 & 2		Average within 10 Working days	5% of periodic Payment
9	Setup of Cloud Environment	2 weeks from PO/LOA	No Delay	5% of one time implementation cost per week delay

Note:

- Periodic Payment means Monthly Payment.
- Days: All Working and Non-working days (365 days in a calendar year)
- 24*7 means three shifts of 8 hours every day. This is applicable for all seven days of the week without any non-working days.
- Severity Levels: Below severity definition, provide indicative scenarios for defining Incidents severity. However, GSTN 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	Production Environment is down or critical malfunction resulting in an inoperative condition or disrupts critical business functions and requires immediate attention.	Non-availability of VM, Storage, API gateway, DB, Internet link and application containers and all security services.
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, The environment is usable but severely limited.	Intermittent network connectivity, UAT and SIT environment.

NOTE:

a) **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.

b) **Scheduled Maintenance** time shall mean the time that the System is not in service due to a scheduled activity. Scheduled maintenance time is planned downtime with the prior permission of the Department, during non-business hours. The Scheduled Maintenance time, within 10 hours a month shall not be considered for SLA Calculation.

c) **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.

d) **Availability means** the time for which the cloud services and facilities are available for conducting operations for the IIM SIRMAUR application running on cloud. Availability is defined as: {(Scheduled Operation Time – System Downtime) / (Scheduled Operation Time)} * 100%

e) **Incident** refers to any event/issue that affects the normal functioning of the services / infrastructure, reported by the IIM SIRMAUR or Users who are using application hosted on the Cloud Service provider (CSP) can be termed as an Incident.

Qualification Criteria

Qualification for Cloud Service Provider (CSP)

#	CSP Mandatory Criteria	Documentary Evidence
1	The Cloud Service Provider (CSP) should have been offering services in India from at least last 3 financial years with average annual turnover of at least Rs. 50 Lakh.	Copy of Certificate of Incorporation or Certified copy of Partnership Deed Letter from Statutory Auditors / Certificate from Chartered Accountant on their letterhead mentioning the annual revenue in India
2	The Cloud Service Provider (CSP) should be empaneled with the Ministry of Electronics & Information and Technology (MEITY), Government of India for offering both DC & DR on its own to government bodies. The CSP Data centers offered for services shall be located in different seismic zone within India.	Undertaking on CSP letterhead confirming the clause and copy of Valid MEITY Empanelment Certificate
3	The CSP's proposed DC & DR center should be operational and live for minimum last 2 years.	Undertaking on CSP letterhead confirming the clause.
4	CSP shall have published on its public/Meity website- cloud services' rates for India, Service Level Agreements (SLAs), dashboard live-status of cloud services' health across global data centre and outage details (if any) with RCA.	An undertaking from the CSP with the links to its relevant public facing website(s) covering the details
5	The proposed Cloud should have Managed cloud native database services for Postgre SQL and My SQL enterprises	Undertaking on CSP letterhead with link to public facing website having the service and functionality description
6	CSP must have their security service in cloud for- • NextGen Firewall • Web Application Firewall • DDoS Protection • Data Encryption at rest • Identity and Access Management - fine grained access control for access to cloud resources: Only the resource with appropriate permissions and grants has access to any specific resource and All access and changes carried out are	Undertaking on CSP letterhead with link to public facing website having the service and functionality description

	logged, cannot be tampered with and be auditable.	
7	Uptime offered on a single VM instance is equal or more than 99.5 %	Undertaking on CSP letterhead with link to public facing website having the service and functionality description
8	• Tier-3 datacenter certification from TIA or equivalent agency (Documentary Evidence-Certificate/) • ISO/IEC 27701:2019 Security techniques —ISO/IEC 27001 • ISO 27017 • ISO 27018 • ISO 9001 • ISO 22301 • PCI-DSS Complied • SOC 1/2/3 Certificate/audited Report • ISO 20000-1	Copy of Relevant Certificate
9	CSP should provide the capability to scale storage automatically without any manual intervention and downtime. This should help customers to pay only for the used capacity rather than unused allocated storage to VM.	Undertaking on CSP letterhead with link to public facing website having the service and functionality description
10	The proposed cloud should provide the latest generation processors with complete flexibility of compute shapes. Customers should have the option to choose any combination of CPU core and memory rather than fixed-sized shapes.	Undertaking on CSP letterhead with link to public facing website having the service and functionality description

Pre-qualification for Managed Service Provider (MSP)

SI. No	Minimum Qualifications Criteria	Documentary proof to be submitted
1.	The Bidder should be – A company incorporated under the Indian Companies Act, 2013 or any other previous company law as per section 2 (20) of the Indian Companies Act 2013/ Partnerships Firm registered under the Limited Liability Partnerships or Partnership Act Registered with the GST Authorities Company should have a valid PAN number	Certificate of Incorporation; and GST Registration certificate issued by GSTN authorities (copy), PAN Card (copy).
2.	The Bidder should have an average annual turnover of at least INR 50 Lakh from IT/ITES services in last three financial years (i.e. FY 2020-21, FY 2021-22 and FY 2022-23).	Duly Audited Financial Statements by the CA or statutory auditor certificate or certificate from Company Secretary of Bidder specifying the net worth for the specified year.
3.	Bidder (MSP) should have following certifications: • ISO9001, • ISO27001, • CMMI Level 3	Copy of certification
4.	Bidder should have executed at least two work order with value of INR 50 lakh each or more from PSU/Central Government /Corporate/Autonomous bodies or similar Institutes/organizations in last 5 financial years to provide Cloud Services.	Copy of Work Orders/Completion certificates duly signed & stamped by the issuing authority.
5.	Bidder has direct reseller authorization with proposed CSP.	Reseller Authorization Certificate from CSP
6.	Bidder has at least 10 technical certified resources (in active employment) for any CSP.	Undertaking from the HR / Copy of Certificate
7.	Submission of “Undertaking of Not Being blacklisted that, the firm or none of the firm’s Partners or Directors have been blacklisted in India by any Indian State / Central Governments Dept. / Public Sector Undertaking of India during last 5 year.	Self-attested Undertaking
8.	Bidder to provide OEM authorization letter/ Manufacturers Authorization Certificate from the MeitY Empaneled OEM quoting this tender reference number, date	OEM Manufacturers Authorization Certificate with empanelment confirmation from MeitY

Other Terms & Conditions:

01. The period of services will be for a period of three years w.e.f. the date of implementation. The Competent authority of this Institute reserves the right to terminate the contract at any point of time by giving one-month notice period.

02. If any dispute arises between the parties, the court for jurisdiction shall be at the Court of Paonta Sahib, Himachal Pradesh only.

03. Payment will be released on the submission of the Original Invoices on monthly basis after TDS deductions as applicable.