Maharashtra Industrial Township Limited (MITL)

RFP for Selection of Service Provider (Cloud Hosting and Managed Service) to Setup, Migrate, and Manage Data Centre (DC) and Disaster Recovery (DR) site for MITL on Cloud

REQUEST FOR PROPOSAL (RFP)

Tender No: MITL/ICT/2026-27/002

Sep 2026

Maharashtra Industrial Township Limited

(MITL)

Udyog Sarathi, MIDC Office, Marol Industrial Area
Andheri (East), Mumbai, Maharashtra, India – 400093

RFP for Selection of Service Provider (Cloud Hosting and Managed Service) to Setup, Migrate, and Manage Data Centre (DC) and Disaster Recovery (DR) site for MITL on Cloud

Ref. no: MITL/ICT/2026-27/002

Sep 2026

Maharashtra Industrial Township Limited (MITL) an SPV between the Maharashtra Industrial Development Corporation (MIDC) and the National Industrial Corridor Development Corporation (NICDC) invites proposals against RFP from interested Bidders for RFP for Selection of Service Provider (Cloud Hosting and Managed Service) to Setup, Migrate, and Manage Data Centre (DC) and Disaster Recovery (DR) site for MITL on Cloud.

The salient features of the project, technical qualification, eligibility criteria and prescribed formats for submission can be accessed in the RFP document uploaded on the website: https://aitl.eproc.in, https://auric.city/

Interested Bidders are requested to submit their online responses to the RFP on or before, 9th Oct 2026, 3:00 PM. Non-refundable processing fee of INR 35,400 (Rupees Thirty-Five thousand Four Hundred only) inclusive of applicable GST shall accompany the submittals through the online portal only on MITL's eproc website as a non-refundable processing fee.

SD/-

Managing Director (MITL)

Instructions to Bidders for e-Tendering

MITL is currently hosting its applications on the Government Community Cloud. The existing cloud infrastructure and managed services have been functioning satisfactorily and are critical for the uninterrupted operation of departmental business applications and digital services.

Now, renew cloud services through the https://aitl.eproc.in platform. Accordingly, MITL intends to renew and continue the Government Community Cloud Hosting and Managed Services through a fresh bidding process on https://aitl.eproc.in , in compliance with the applicable procurement norms and guidelines.

Therefore, MITL invites bids from eligible and qualified bidders to provide “Government Community Cloud Hosting & Managed Services” for the continued hosting, management, maintenance, monitoring, and support of MITL’s business applications and associated infrastructure.

Any communication related to the tender must be sent to the following address:

To
Managing Director,
Maharashtra Industrial Township Limited
Udyog Sarathi E, MIDC Office,
Marol Industrial Area, Andheri (East)
Mumbai, Maharashtra State, India – 400093

Definition :- Managed Service Provider and Cloud Service Provider

For the purposes of this RFP and the Contract arising from it, the Managed Service Provider ("MSP") and the Cloud Service Provider ("CSP") shall be one and the same legal entity. The Bidder shall itself be the Cloud Service Provider empanelled with the Ministry of Electronics and Information Technology (MeitY) under the Government Community Cloud (GCC) category, and shall itself deliver the managed services set out in this RFP from its own MeitY-empanelled data centres.

Accordingly, wherever this RFP uses the expressions "MSP", "CSP", "CSP/MSP", "Service Provider" or "Successful Bidder", each such expression shall be read as referring to the same single entity, and every obligation, eligibility requirement, service level, penalty and liability stated against any one of those expressions shall bind that entity in full.

Bids submitted as a consortium, joint venture, or on a prime-and-subcontractor basis in which the managed services and the underlying cloud infrastructure are provided by different legal entities, shall not be accepted. This clause does not apply to the Master System Integrator (MSI) or the e-LMS System Integrator (SI) referred to in Section 10.3, who are separate parties appointed by the Client and are not part of the MSP/CSP scope.

1. Accessing/Purchasing of RFP documents

(i) It is mandatory for all the bidders to have a class-III Digital Signature Certificate (DSC) (with both DSC components, i.e. signing and encryption in the name of authorized signatory who will sign the RFP response) from any of the licensed Certifying Agencies (Bidders can see the list of licensed CAs from the link https://aitl.eproc.in to participate in e-tendering of the Client).

(ii) DSC should be in the name of the authorized signatory as authorized in the submitted Proposal. It should be in corporate capacity (that is in Bidder capacity). Please ensure the submission of document certifying the Class III DSC.

(iii) To participate in the RFP, it is mandatory for the Bidder to register their firm with e-tendering portal of the Client, to have user ID & password which has to be obtained by submitting the applicable fee & necessary documents. Validity of online registration is one year. Following may kindly be noted:

(a) Registration should be valid at least up to the date of submission of Proposal;

(b) Proposals can be submitted only during the validity of their registration.

(c) The amendments / clarifications to the RFP document, if any, will be hosted on the Client's website. https://aitl.eproc.in ; https://auric.city

(d) If the firm is already registered with e-tendering portal of Client and validity of registration is not expired the firm / Joint Venture is not required a fresh registration.

(iv) The complete RFP document can be viewed / downloaded from e-tender portal of Maharashtra Industrial Township Limited, from the date & time mentioned in the Data Sheet.

2. Preparation & Submission of Proposals

The bidders may submit his Proposal online following the instructions appearing on the screen. A buyer manual containing the detailed guidelines for e-procurement is available on e-procurement portal:

(i) The documents shall be prepared and scanned in different files (in PDF or JPEG format such that file size is not more than 10 MB) and uploaded during the on- line submission of Proposal.

(ii) Proposal must be submitted online only through e-procurement portal of the Client, using the digital signature of authorized representative of the Bidder on or before the Proposal Due Date mentioned in the Data Sheet.

3. Modification / Substitution / Withdrawal of Proposals

(i) The bidder may modify, substitute or withdraw its e- Proposal after submission prior the Proposal Due Date. No Proposal shall be modified, substituted or withdrawn by the Bidder on or after the Proposal Due Date & Time.

(ii) Any alteration / modification in the Proposal or additional information supplied subsequent to the Proposal Due Date, unless the same has been expressly sought for by the Client, shall be disregarded.

(iii) For modification of RFP, bidder has to detach its old Proposal from e-tendering portal and upload / resubmit digitally signed modified Proposal.

(iv) For withdrawal of Proposal, bidder has to click on withdrawal icon at e-tendering portal and can withdraw its e-Proposal.

(v) It may specifically be noted that once a proposal is withdrawn for any reason, a bidder cannot re-submit the e-Proposal.

4. Opening & Evaluation of Proposal

(i) Opening and evaluation of the proposal will be done through an online process.

5. Submission of Hard Copy Documents

1. The bidder shall submit only the Power of Attorney and the Earnest Money Deposit (EMD) in the form of a Demand Draft (DD), as specified in this document, to the MITL Head Office.

   Mention the Tender Name on the envelope: **"RFP for Selection of Service Provider (Cloud Hosting and Managed Service) to Setup, Migrate, and Manage Data Centre (DC) and Disaster Recovery (DR) site for MITL on Cloud"**

6. Tender Fee Payment:

The bidder shall remit the applicable Tender Fee to the bank account specified below and upload the payment receipt/proof of payment on the MITL e-Procurement Portal (https://aitl.eproc.in) along with the bid submission.

Beneficiary Name: Maharashtra Industrial Township Limited

Address: Udyog Sarathi, MIDC Office, Andheri (E), Mumbai – 93

Name of the Bank: Bank of India

Branch address: Chakala Branch, Andheri (East)

Type of Account: Current Account

Account No: 006720110000968

IFSC Code: BKID0000067

Disclaimer

1. This RFP document is neither an agreement nor an offer or invitation by the Maharashtra Industrial Township Limited (MITL) to the prospective bidders or any other person. The purpose of this RFP is to provide information to the interested parties that may be useful to them in the formulation of their proposal pursuant to this RFP.
2. MITL does not make any representation or warranty as to the accuracy, reliability or completeness of the information in this RFP document and it is not possible for MITL to consider particular needs of each party who reads or uses this RFP document. This RFP includes statements which reflect various assumptions and assessments arrived at by MITL in relation to the RFP. Such assumptions, assessments and statements do not purport to contain all the information that each bidder may require. Each prospective bidder should conduct its own investigations and analyses and check the accuracy, reliability and completeness of the information provided in this RFP document and obtain independent advice from appropriate sources.
3. MITL will not have any liability to any prospective Firm/ or any other person under any laws (including without limitation the law of contract, tort), the principles of equity, restitution or unjust enrichment or otherwise for any loss, expense or damage which may arise from or be incurred or suffered in connection with anything contained in this RFP document, any matter deemed to form part of this RFP document, the award of the Assignment, the information and any other information supplied by or on behalf of MITL or their employees, any consultants or otherwise arising in any way from the selection process for the Assignment. MITL will also not be liable in any manner whether resulting from negligence or otherwise however caused arising from reliance of any Bidder upon any statements contained in this RFP.
4. MITL will not be responsible for any delay in receiving the proposals. The issue of this RFP does not imply that MITL is bound to select a bidder and MITL reserves the right to accept/reject any or all of proposals submitted in response to this RFP document at any stage without assigning any reasons whatsoever. MITL also reserves the right to withhold or withdraw the process at any stage with intimation to all who submitted the RFP Application.
5. The information given is not an exhaustive account of statutory requirements and should not be regarded as a complete or authoritative statement of law. MITL accepts no responsibility for the accuracy or otherwise for any interpretation or opinion on the law expressed herein.
6. MITL reserves the right to change/ modify/ amend any or all provisions of this RFP document. Such revisions to the RFP / amended RFP will be made available on the website of MITL.
7. This RFP including the selection process shall be governed by, and construed in accordance with, the laws of India and the Courts at Mumbai shall have exclusive jurisdiction over all disputes arising under, pursuant to and/or in connection with the Selection Process.
8. The Client, in its sole discretion and without incurring any obligation or liability, reserves the right, at any time, to:
    a) Suspend and/or cancel the Selection Process and/or amend and/or supplement the Selection Process or modify the dates or other terms and conditions relating thereto;
    b) Consult with any Bidder in order to receive clarification or further information;
    c) Retain any information and/or evidence submitted to the Client by, on behalf of and/or in relation to any Bidder; and/or
    d) Independently verify, disqualify, reject and/or accept any and all submissions or other information and/or evidence submitted by or on behalf of any Bidder.

TENDER NOTICE

Sealed Tenders are invited for RFP for Selection of Service Provider (Cloud Hosting and Managed Service) to Setup, Migrate, and Manage Data Centre (DC) and Disaster Recovery (DR) site for MITL on Cloud. Tenderers must be reputable organisations with relevant experience.

Sr.	Tender No.	MITL/ICT/2026-27/002
1	Name of Work	RFP for Selection of Service Provider (Cloud Hosting and Managed Service) to Setup, Migrate, and Manage Data Centre (DC) and Disaster Recovery (DR) site for MITL on Cloud
2	Tender Fee	Non-refundable Rs. 35,400 (Rupees Thirty Five Thousand Four Hundred only) including GST
3	Bid Security (EMD)	Rs.10,00,000/- (Rupees Ten Lakh Only)
4	Address for Correspondence	Managing Director, Maharashtra Industrial Township Limited Udyog Sarathi E, MIDC Office, Marol Industrial Area, Andheri (East) Mumbai, Maharashtra State, India – 400093
5	Details for Downloading Tender Document	The complete RFP document can be viewed/downloaded from website of https://aitl.eproc.in, www.auric.city
6	Submission of Bid	Bid must be submitted online only at (https://aitl.eproc.in) on or before (up to 9th Oct 2026 by 3:00 PM (at 1500 hours IST)).
7	Email address for Pre-Bid Queries	Mr. Sadashiv Lokhande (Manager-IT) E- Mail- managerit@mitl.org.in Ph -9850535018 Mr.Sagar Paraswar (Manager- Infra and Planning) E-Mail- managerinfrahq@mitl.org.in Ph- 9860728933

The details of tender schedule are as below:

S. No.	Event Description	Date
1	Date of issue of RFP	18th Sep 2026
2	Last date for receiving queries	22nd Sep 2026
3	Pre-Bid Meeting	23rd Sep 2026
4	The Employer's response to queries	24th Sep 2026
5	Last Date of submission of Proposals	9th Oct 2026 by 3:00 PM
6	Date of Opening of Technical Proposal	9th Oct 2026 at 4:00 PM
7	Date of Opening of Financial Proposal	To be notified to Bidders
8	Announcement of Technically Qualified Bidders	To be notified to Bidders
9	Opening of Financial Proposal	To be notified to Bidders
10	Letter of Award (LOA)	To be notified to Bidders
11	Signing of Contract	Within 10th days from LOA

Contents

1 Introduction

The Government of India is undertaking various industrial corridor projects under the National Industrial Corridor Development Programme (NICDC). This initiative aims to establish forward-looking industrial cities in India that can compete on a global scale in manufacturing and investments. These projects are expected to generate job opportunities and foster economic growth, contributing to overall socio-economic development. According to NICDC, the National Infrastructure Pipeline includes 32 projects in 4 phases across 11 corridors. One such project is the freight corridor connecting the National Capital Region of Delhi and Jawaharlal Nehru Port in Mumbai. This freight corridor passes through states such as Uttar Pradesh, Madhya Pradesh, Haryana, Rajasthan, Gujarat, and Maharashtra and is being developed as the Delhi-Mumbai Industrial Corridor (DMIC). This freight corridor spans 1483 km in length, with an influence region extending about 150 km on either side to harness its developmental potential. NICDC and Maharashtra Industrial Development Corporation (MIDC) under the SPV of Maharashtra Industrial Township Limited (MITL) ('The Client').

MITL has 51% stake of MIDC and 49% stake of NICDC. MITL will also have the status of a Special Planning Authority (SPA) and will be responsible for the development, management, and operations of all nodes within Maharashtra.

The overall vision of MITL includes positioning of Information & Communications Technology (ICT) as the key enabler to integrate various functions of the city development and operations, provide advanced and affordable services to the citizens, along with efficient governance and management of the city operations. ICT will enable the creation of a sustainable ecosystem of the government, industries/businesses, and social infrastructure with an overall citizen-centric development. It will also enable MITL to be an efficient and tech-savvy organisation that will truly leverage ICT for its operations and decision-making. ICT will cultivate the development of a digital and connected city, which ultimately helps in promoting and sustaining economic growth and development.

Maharashtra Industrial Township Limited (MITL) intend to issue this RFP (Request for Proposal), to eligible bidders, to participate in the competitive bidding through https://aitl.eproc.in for appointment of a Cloud service provider (CSP) for providing 'Government Community Cloud Hosting & Managed Services.

For this purpose, MITL invites proposals for undertaking the activities mentioned under the Project Scope; for procuring 'Government Community Cloud Hosting & Managed Services for MITL.

1.1 Project Objective:

The objective of this RFP is to enable Maharashtra Industrial Township Limited (MITL) to set up and manage its applications on the cloud. MITL wish to engage a single entity to provide and manage Cloud Services for a period of 26 months. Further, the contract may be extended based on mutually agreed terms and conditions between MITL and the selected bidder, subject to satisfactory performance and in accordance with the provisions and conditions specified in this RFP.

MITL intend to appoint a Cloud Service Provider (CSP). The primary responsibility of CSP shall be to host and manage MITL applications on a MeitY empanelled Cloud Platform/Cloud Service Provider. CSP shall assume total responsibility for the entire scope of work and will be held liable for any delays, performance, quality, and other issues.

1.2 Project Scope

The broad scope of the project includes engagement of a single service provider for providing Government Community Cloud Hosting and comprehensive managed services for the cloud infrastructure required for departmental business applications.

MITL intends to procure "Government Community Cloud Hosting & Managed Services" through the https://aitl.eproc.in portal for hosting and management of its business applications. The selected

bidder/service provider shall provide Government Community Cloud Hosting along with complete managed services under this bidding process for an initial period of 26 (Twenty-Six) months.

Further, the contract may be extended based on mutually agreed terms and conditions between MITL and the selected bidder, subject to satisfactory performance and in accordance with the provisions and conditions specified in this RFP.

The proposed solution shall be highly configurable, secure, highly responsive and shall support integration and optimization of required services and solutions used by MITL.

The broader requirements are expressed in the below –

- Cloud Infrastructure for Application Hosting.
- Migration of all MITL applications from existing Cloud to the new Cloud environment
- End to End Managed Service

Summary of Applications which will be hosted on the Cloud are given below:

Component	Project requirement	Make
Existing System Components		
e-Land Management System (e-LMS)	e- Land Management System (e-LMS) is already under operations for allotment and management of land in AURIC. The system shall be migrated from the current cloud environment and subsequently hosted on the cloud by the CSP in coordination with the SI.	Bespoke
MITL Website	There is an existing website www.auric.city and www.mitl.org.in which is being used to provide essential information to citizens and stakeholders. The system shall be migrated from the current cloud environment and subsequently hosted on the cloud by the CSP in coordination with MSI.	Bespoke
AURIC e-Governance and ERP (AEE)	Following data will be hosted on cloud by the CSP: • **Customer Facing Systems**: Portal, E-governance functions, M-Governance Functions, Social Governance, Web based GIS layer, Digital Locker, citizen smart card, Mobile Applications, Birth and Death module, Trade License Module, RTI Module, Legal Module, Citizen Grievance Redressal Module, Automated Building Plan Approval System (BPAS), Management Information System along with KPI and Dashboards etc.; **All the above systems are already under operations in their current Cloud environment and shall be migrated and subsequently hosted on the cloud by the CSP in coordination with MSI**	• Bespoke for e-Governance System • ESRI for GIS • ERP System. • BPAS.
GIS- CDCPR	GIS- CDCPR and AD servers	ESRI and CDCPR
Electricity Procurement	Electricity procurement application	(Mercodose)

Component	Project requirement	Make
Utility Billing Software	Integrated utility billing system	Bespoke
Other's	Others system	

1.3 Purpose of RFP

MITL intends to issue this tender document to eligible bidders to participate in the competitive bidding for the appointment of an CSP for providing Government Community Cloud Hosting & Managed Services. The proposed solution shall be highly configurable, secure, and very highly responsive and shall support integration and optimisation of required services and solutions used by the MITL.

1.4 Requirement of Cloud Services

As part of IT initiatives, MITL has implemented various IT Applications which are currently hosted on the Government Community Cloud. MITL need to renew existing Cloud services. MITL intends to appoint a Cloud Service Provider to provide Cloud Hosting and Managed Services. The CSP shall follow the compliance requirements below:

1. MeitY has empaneled the Cloud Service offerings of CSPs in the form of a Bouquet of Cloud Services. Cloud Platform/ Cloud Service Provider proposed by CSP should be empaneled with MeitY.
2. The proposed cloud platform/CSP, along with its associated data centre, which shall host MITL application, shall be clearly mentioned as part of the bid. Only the STQC audited data centres as mentioned on the https://ambud.meity.gov.in/empaneledCsp shall be proposed.
3. CSP shall offer cloud services with their Data Centre location within India only. All the physical servers, storage, and other IT hardware from where cloud resources are provisioned for MITL must be within the Indian Data Centre only. CSP shall ensure that MITL data resides within India only. All monitoring and provisioning should be within India and 100% isolated from other regions outside India, if in case CSP has a global presence.

1.5 Earnest Money Deposit

1. An Earnest Money Deposit(EMD) in the form of a Bank Guarantee in format provided in Prequalification Criteria Document, from a scheduled Indian Bank in favour of 'Maharashtra Industrial Township Limited', valid for 180 (one hundred and Eighty) days from the PDD, payable at Mumbai, for the sum of Rs.10,00,000/-(Rupees Ten Lakh Only) shall be required to be submitted by each Bidder("EMD"). A scanned copy of the same shall be uploaded by Bidder in the online bid and a hard copy of the same will have to be submitted at MITL Mumbai Office before the bid submission time.
2. Unsuccessful Bidder's EMD will be returned as promptly as possible after the opening of the Price Bid.
3. The EMD may be forfeited:

1. If Bidder (i) withdraws its e-Bid during the period of e-Bid validity specified by the Bidder on the e- bid form: or (ii) does not accept the correction of errors or (iii) modifies its e-Bid price during the period of e-Bid validity specified by the Bidder on the form.
2. In case of a successful Bidder, if the Bidder fails to sign the contract with the MITL.

2 ELIGIBILITY AND TECHNICAL EVALUATION CRITERIA

2.1 ELIGIBILITY CRITERIA

#	Basic Requirement	Eligibility Criteria	Document to be submitted
1	Legal Entity	The CSP should be a Legal Entity registered under the Companies Act, 2013 or the Companies Act, 1956 OR a Limited Liability Partnership (LLP) registered under the LLP Act, 2008 or Indian Partnership Act 1932.	Copy of Certificate of Incorporation/Registration/Partnership deed
2	Meity Empanelment	a. The CSP should be MeitY empaneled (as on bid submission date) b. The proposed Data Centre should be within India. c. The proposed Data Centre should be successfully STQC audited. d. The proposed Data Centre should have a running Government Community Cloud (GCC). e. The CSP should be the single point of contact for the entire migration (if demanded) and providing Cloud services for the entire contract period.	Valid copies of proof attested by authorized Bid signatory
3	Compliance	The CSP is compliant with IT Act 2000 (including 43A) and amendments	Letter from authorized signatory on the letter head of bidder mentioning the compliance.
4	Turnover	A CSP should have a minimum average annual turnover of at least 150 Crore in last three audited financial years (FY 2022–23, FY 2023–24, and FY 2024–25.)	Certificate from the Statutory Auditor/Chartered Accountant
5	Net worth	The CSP should have a positive net worth as on 31st March, 2025.	Certificate from the Statutory Auditor/Chartered Accountant
6	Blacklisting	The CSP should have never been debarred/ blacklisted by any Government/PSU/State Agency/Government undertaking in India till the date of submission.	Letter signed by the Authorized in format given in the RFP.

#	Basic Requirement	Eligibility Criteria	Document to be submitted
7	Data Centre Facility	The Data Centre & DR site should be at least Tier III standard (certified under TIA 942 or Uptime Institute certifications) and implement processes based on ITIL standards. Primary Site should be in Maharashtra (preferably in Mumbai/Navi Mumbai region)	Valid copy of the certificate
8	Data Centre Certification	Certification; o ISO 27001-2022, ISO/IEC 27701:2019 o ISO/IEC 27017:2015-Code of practice for information security for cloud services and Information technology. o ISO 27018-2019 - Code of practice for protection of personally identifiable information (PII) in public clouds. o ISO 14001:2015 o ISO 9001:2015 o ISO-22301-2019 for Business Continuity Management. o ISO-20000-1:2018 o PCI DSS - compliant infrastructure for processing the financial transaction in the cloud.	Valid copies of the certificate
9	Data Centre	The CSP must be operating in multiple MeitY GCC empanelled Data Centres in India. CSP should have minimum two MeitY empanelled data centres for services like DC,DR and NDR/DR2 (In case required in the future)	Letter from Authorised signatory on the letterhead of the bidder.
10	Capability	The CSP should have successfully implemented/commissioned at least five (05) projects of DC/DR with Cloud Deployment on Government Community Cloud (GCC) with order value of at least 5 Cr. each	Work order/contract
11	Manpower Strength	The CSP must have the strength of at least 200 IT Professionals (data centre /networking/system administration/ cloud services professionals/cloud security experts) on their payroll as on the date of submission of this bid. At least 50 of these cloud professionals must have in deployment and Management of cloud solution/ DR Management / virtual server	Certificate jointly signed by HR Head and Director / Partner / Person Authorised to submit Bid.

#	Basic Requirement	Eligibility Criteria	Document to be submitted
		administration/system administration, Virtualization, security, database, etc.)	
12	Pre-Qualification Cover letter	Acceptance of Scope of Work and Term & Conditions mentioned in Bid Document	Undertaking from CSP on letterhead from the authorized signatory
13	Advance Security	The CSP should have accreditations relevant to security, availability, confidentiality, processing integrity, and/or privacy Trust Services principles -SOC 1, SOC 2.	A valid copy of the certificate/Report

Bids submitted as a consortium, joint venture, or on a prime-and-subcontractor basis in which the managed services and the underlying cloud infrastructure are provided by different legal entities, shall not be accepted. This clause does not apply to the Master System Integrator (MSI) or the e-LMS System Integrator (SI) referred to in Section 10.3, who are separate parties appointed by the Client and are not part of the CSP scope.

Note:

1. Supporting documents requested should be arranged / numbered in the same order as mentioned above.
2. Failure to meet any of these criteria will disqualify the applicant.
3. MITL reserves the right to verify and/ or to evaluate the claims made under Pre-Qualification criteria and any decision in this regard shall be final, conclusive,and binding upon the company.
4. All certificates or documents should also be self-attested and attached together. If at a later stage it is found that bidder has provided false information or has wrongly certified the conditions stated in the Pre-Qualification criteria, the bidder shall be liable for action as per Attachment 1- Corrupt and Fraudulent Practices of “Special Terms and Conditions of Contract” document.

2.2 Technical Evaluation Criteria

The technical proposal shall be evaluated based on the following technical evaluation criteria as of the last date of submission of this bid. Minimum marks for Qualification in Technical Evaluation Criteria shall be 70 Marks.

S. No	Type	Qualification Criterion	Documentary Evidence	Marks Allocated	Max Marks
1.	**Company Financials & Profile**	The Bidder should have minimum average annual turnover of at least 150 Crore in last three audited financial years (FY,2022-2023,2023-2024,2024-2025)	Audited financial statements for last three Financial Years, OR Statutory auditor's certificate OR CA Certificate clearly specifying turnover	150 - 250cr: 10 Marks >250cr: 20 Marks	20
2.	**Manpower Strength**	The CSP must have the strength of at least At least 50 of these cloud Solution Architects/ professionals must have in deployment and Management of cloud solution / DR Management / virtual server administration/ system administration, Virtualization, security, database, etc.)	Certificate jointly signed by HR Head and Director / Partner / Person Authorised to submit Bid.	50 to 100- 1 Marks 100 to 150 - 3 marks >150 – 5 marks	5
3.	**MeitY empanelled Cloud Services under the Government Community Cloud**	Number of Data Centres in India from where the MeitY empanelled Cloud Services are offered under the Government Community Cloud	Valid copies of proof attested by authorized Bid signatory	Two locations – (5 Marks); Three locations – (10 Marks); Four or more locations – (15 Marks)	15
4.	**Certifications**	The CSP should hold valid certifications for the following standards: 1. ISO 9001 2. ISO/IEC 27001, 3. ISO 22301, 4. SOC 3, 5. ISO/IEC 20000-1,	Valid copies of Certificates attested by authorized Bid signatory	(a) 1 mark per certificate — max 7 marks. (b) ISO/IEC 42001:2023 — 3 marks.	10

S. No	Type	Qualification Criterion	Documentary Evidence	Marks Allocated	Max Marks
		6. ISO/IEC 27017, 7. ISO/IEC 27018, 8. ISO/IEC 42001:2023			
5.	**Cloud Project Experience**	The Bidder have successfully completed/Ongoing/ Currently hosted Data Centre/ Disaster recovery Cloud Services on Government community cloud for any Govt. organization / PSU with order value of at least 5 Cr. each in last five financial years.	Work order/LOI	5 Projects- 5 Marks >5 Projects – 10 Marks	10
4.	**ERP Project Experience**	The Bidder must have successfully completed OR be currently providing hosting and managed services for a minimum One (1) COTS (Commercially off the Shelf) ERP System i.e SAP based or Oracle based System on the proposed Cloud Platform with a contract value of not less than INR 3 Crore for any Govt. organization/ PSU in India in last five years.	Work Order, Purchase Order (PO), OR Letter of Intent (LoI), along with relevant extracts from the signed contract clearly indicating the project value and scope of work. AND Completion Certificate/Go-Live Certificate issued by the client, OR invoices evidencing payment received for the services rendered.	1-3 Projects- 5 Marks >3 Projects – 10 Marks	10
5	**Presentation**	Technical Presentation based on Methodology and Process for overall implementation of projects. The bidders shall be evaluated on the following aspects: • Understanding of Scope of Work	Copy of Presentation to be submitted	30	30

S. No	Type	Qualification Criterion	Documentary Evidence	Marks Allocated	Max Marks
		• Approach & Methodology • Implementation Strategy • Complexity of software • Project Plan / Timelines			
Total Marks					**100**

Only those bidders who secure a minimum of 70 marks (70%) or above in the Technical Qualification evaluation shall be declared technically qualified, and the Financial/Commercial Bids of only such technically qualified bidders shall be opened for further evaluation under the QCBS methodology. Bidders scoring below 70 marks shall be treated as technically disqualified, and their Commercial Bids shall not be opened.

2.3 Opening of Commercial Bids

1. Only those bidders, who have scored at least 70% marks in technical bid evaluation process shall be declared as “Technically Qualified Bidders”.
2. The Commercial Bids of only “Technically Qualified Bidders” will be opened. The decision of the MITL’s in this regard shall be final.
3. The Commercial Bids will be opened, in the presence of Bidders’ representatives (Maximum two for each bidder). Attendance for Commercial Bids opening is not mandatory for the bidders. The bidder’s representatives who are present shall sign a register evidencing their attendance.
4. The Bidders are required to quote for all the items as mentioned in the Price Schedule. Therefore, any Bid which does not quote for all the items will be determined to be non-responsive and will be rejected.

2.4 Bid Evaluation

The technical Bids, along with all the supporting documents, shall be submitted through the online portal. The department will review the technical bids of the CSP to determine whether the technical bids are substantially responsive.

2.4.1 Technical Evaluation

All bids received will first be evaluated against the prescribed Pre-Qualification (PQ)/Eligibility Criteria. Only those bidders who meet all technical and eligibility requirements will be declared technically qualified.

Bids that are not substantially responsive are liable to be disqualified at department's discretion. The CSP's technical solutions proposed in the bid document will be evaluated as per the requirements specified in the RFP and technical evaluation framework. The Bidder would be required to cover the following but not limited to:

- Overall Cloud architecture.
- Cloud Security Solution.
- Migration Strategy
- SLA Management.
- Business continuity Management.
- Managed Services.

The evaluation process will be conducted in two stages — Technical Evaluation and Commercial Evaluation.

All bids received will first be evaluated against the prescribed Pre-Qualification (PQ)/Eligibility Criteria. Only those bidders who meet all technical and eligibility requirements will be declared technically qualified.Bids that are not substantially responsive are liable to be disqualified at department's discretion. The CSP's technical solutions proposed in the bid document will be evaluated as per the requirements specified in the RFP and technical evaluation framework. The Bidder would be required to cover the following but not limited to:Overall Cloud architecture.

- Cloud Security Solution.
- Migration Strategy
- SLA Management.
- Business continuity Management.
- Managed Services.

The evaluation process will be conducted in two stages — Technical Evaluation and Commercial Evaluation.

2.5 Award of Contract

The bid shall be evaluated on the Quality and Cost Based Selection (QCBS) methodology, with a weightage of 70% to the Technical bid and 30% to the Commercial bid. The contract shall be awarded to the bidder securing the highest Composite Score (H1), subject to fulfilment of all terms and conditions specified in this RFP. The detailed QCBS methodology and formulae are set out below

- Under QCBS selection, the technical bids will be allotted weightage of 70% and while the commercial bids will be allotted weightages of 30%.
- The bid with the highest technical score shall be given a score of 100 and other bidders technical proposal scores that are proportional to their marks with respect to the highest technical marks.
- The bid with the lowest cost will be given a commercial scope of 100 and other bidders commercial scores that are inversely proportional to their prices with respect to the lowest offer.
- The total score, both technical and commercial, shall be obtained by weighing the quality and cost scores and adding them up. On the basis of the combined weighted

score for quality and cost, the bidders will be ranked in terms of the total score obtained.

- The bid obtaining the highest total combined score in evaluation of quality and cost will be ranked as H1 followed by the bid securing lesser marks as H2 and H3 etc.
- The bid securing the highest combined marks and ranked H1 will be invited for negotiation, if required and shall be recommended for award of contract. In the event two or more bids have the same score in final ranking, the bid with highest technical score will be ranked as H1 and will be invited first for negotiations.
- An evaluated bid score (B) will be calculated for each responsive bid using the following formula, which permits a comprehensive assessment of the bid price and the technical merits of each bid.

Evaluated bid score (B) = (T/T high*70) + (C low/C*30)

Where,

- C – Evaluated Bid price
- C Low – The lowest of all evaluated bid prices among responsive bid
- T – The technical score awarded to the bid
- T high – the technical score achieved by the bid that was scored best among all responsive bids.

Bidder	Technical Marks	Commercial Marks	Calculation of bid score	Evaluated Bid score (B)	Rank
1	88	110	[88/95*70] + [110/110*30]	94.84	H-2
2	90	140	[90/95*70] + [110/140*30]	89.88	H-3
3	80	160	[80/95*70] + [110/160*30]	79.57	H-4
4	95	130	[95/95*70] + [110/130*30]	95.38	H1

2.6 Notification of Award

Prior to expiry of the validity period, the MITL will notify the “Successful Bidder”.

The “Successful Bidder” shall furnish a “Performance Security” in the form of a Performance Bank Guarantee (“PBG”) from a Scheduled or Nationalized Bank in the prescribed format within 10 working days (i.e., excluding bank holidays) of receipt of the notification of award from the MITL.

2.7 Performance Bank Guarantee

Performance Bank Guarantee (PBG) of value of 10% of Contract Value need to be provided by the successful bidder as per the format given in RFP. PBG should be drawn on Nationalised / Scheduled Bank for 26 Months with additional claim period of 1year from the date of expiry providing for encashment at Mumbai Branch.

2.8 Signing of Agreement

On receipt of PBG from the Successful Bidder along with the signed copies (two nos.) of the agreement on stamp paper (As per Rule) from the Successful Bidder, both parties shall sign the Contract agreement within 15 days of issuing of LOA.

3 Scope of Work

MITL is currently hosting its applications on the Government Community Cloud. The existing cloud infrastructure and managed services have been functioning satisfactorily and are critical for the uninterrupted operation of departmental business applications and digital services.

Now, renew cloud services through the departmental e-bidding platform https://aitl.eproc.in. Accordingly, MITL intends to renew and continue the Government Community Cloud Hosting and Managed Services through a fresh bidding process on https://aitl.eproc.in, in compliance with the applicable procurement norms and guidelines.

3.1 Managed Services

The following broad areas of services are envisaged under this project:

3.1.1 Design of cloud infrastructure

1. CSP shall set up and manage the entire cloud solution deployed for MITL by Provisioning and managing cloud-based resources on a subscription-based / OPEX Model only.
2. CSP shall host MITL applications on Government Cloud Community (GCC).
3. Applications for customers/ citizen shall be hosted in public domain i.e. DMZ and databases shall be hosted in MZ zone.
4. CSP shall provide a detailed solution document for setting up of the Infrastructure. The same shall be approved by the MITL representative.
5. Subsequently, the CSP shall provision the entire infrastructure (compute, storage, network, security, software, bandwidth etc.) required for setting up of the site as per the requirement.
6. CSP shall 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. There should not be any constraints on the services.
7. The CSP shall ensure that all peripherals, accessories, sub-components required for the functionality and completeness of the solution, including but not limited to devices, equipment, accessories, software, licenses, tools, etc. should also be provisioned according to the requirements of the solution.
8. The MITL will not be responsible if the CSP has not provisioned some components, subcomponents, assemblies, and sub-assemblies as part of the bill of materials in the bid. The CSP will have to provision the same to meet the solution requirements at no additional cost and time implications to MITL.
9. The Cloud services shall be available on pay as per usage model.

3.1.2 Deployment of solution on Government Community Cloud (GCC)

- The GCC shall be hosted on a separate isolated cloud at the CSP's Data Centre as opposed to other community cloud.
- GCC shall only host Cloud services for Departments / Ministries / Agencies / Autonomous Institutions / Statutory Bodies / Offices under Government of India or States or UTs or Local Governments or PSUs within India (herein after referred to as Government Departments).

- The space allocated for the GCC infrastructure should be clearly demarcated and identified as hosting Government Departments projects. The demarcated and identified area shall not host any components other than those of Government Departments projects.
- The infrastructure elements including physical server, physical storage (including backup storage) and network equipment in the GCC shall be dedicated only for the Government departments. There shall be physical and logical separation (of space, servers, storage, network etc.) from the public and other cloud offerings of the Cloud Service Provider. However, these infrastructure elements can be shared (physically only) among the Government Departments within GCC only.
- The entire Network Path for each of the hosted MITL applications shall be logically separate from that of other government MITL.
- The entire Network path of us shall be administered through a Firewall with secured VLAN zoning.
- CSP shall administer the Firewall policy as per MITL's directions. The CSP shall also enable MITL to administer the firewall policy remotely. CSP shall also provide read-only access of the firewall configuration to authorised personnel of MITL.
- With respect to monitoring tools, if any agent has to be deployed on the VMs or otherwise, the monitoring tools may be shared provided there is logical segregation and controls built- in to ensure that the tools & deployed agents comply to the security policies and only the events, performance threshold alerts and inventory data for the OS, DB, infrastructure and Application is captured & sent by the deployed agents. The monitoring tools and deployed agents (in case of agent-based tools) shall not capture or send Government MITL application and/or user and/or transaction data.

3.1.3 Infrastructure Analysis and Build

CSP shall provide complete infrastructure details at cloud site including following parameters

- CPU provision/utilization
- RAM provision/utilization
- Disk provision/utilization
- Network interface requirement
- Network throughput requirement
- Backup provision/utilization

Proposed Solution should be compatible with IPv6 and High-level architectural diagram showing different layers of solution like Internet / P2P Connectivity, Network, Security, Compute, Hardware, Storage & Backup layers.

CSP should propose to deploy different applications and database in different VLANs with restricting users to directly access database layer and storage layer.

CSP shall provide Backup solution with different features, like snapshots of VMs, RDBMS backup, incremental and full back up of all data, restoration of data in test environment or as and when required.

Backup & Restore Service

- CSP shall provide backup solution (Disk / Tape based backups), covering but not limited to daily, weekly, monthly, quarterly and annual backup functions (full volume and incremental) for data and software maintained on the servers and storage systems using Enterprise Backup Solution.

- CSP shall cover (not limited to) Backup & Restoration of VM images, Operating System, Applications, Databases and File system etc.
- CSP shall Configure, schedule, monitor and manage backups of all the data including but not limited to files, images, and databases as per the policy/procedure/plan finalized by department.
- CSP shall also perform Administration, tuning, optimization, planning, maintenance, and operations management for backup and restore.
- The disk-based backup solution must have the feature to integrate with any Tape Library.
- CSP should propose cloud native solution or use a SaaS based/Third Party Software deployed on VM based backup software.
- The Long-Term Storage should have an option of enforcing WORM (Write Once, Read Many) policy for section of data that requires the same.
- Department should be able to recover individual files, complete folders, entire drive or complete system to source machine or any other machine available in network.
- CSP shall restore the requested data with the objective to initiate a minimum of 95 percent of the total number of restore requests per calendar month for data that can be restored from a local copy.
- CSP shall Provide and install additional infrastructure capacity for backup and restore.
- There has to be provision if required to shift the backup at department required location on tape/USB.
- CSP shall perform restoration testing biannually with the permission of department.
- CSP must ensure integrity of the data returned during a restore by verifying the block data read with a check sum of the data.
- CSP shall ensure prompt execution of on-demand backups & restoration of volumes, files and database applications whenever required.
- CSP shall perform Real-time monitoring, log maintenance and reporting of backup status on a regular basis. Prompt problem resolution in case of failures in the backup processes.
- The backup service must provide following capabilities.
- Compression: Support compression of data at source before backup
- Encryption: Support at least 128-bit encryption at source
- Alert: Support email notification on backup job's success / failure
- File exclusion: Ability to exclude specific files, folders, or file extensions from backup
- Deduplication: Provide deduplication capabilities
- Backups should be stored in such a way that disaster should not result in loss of backups.

Indicative Backup plan

#	Backup Type	Backup Frequency	Retention Period
1	Incremental	Daily	7 Days
2	Full	Weekly	1 Month
3	Full	Monthly	12 Months
4	Full	Yearly	7 Years

3.1.4 Dynamic Scaling of Resources

- The initial sizing & provisioning of the underlying infrastructure (including the system software and bandwidth) shall be carried out as per the actual requirement of department.

- Department will select and provide the details of the services required as and when required by the department.
- Subsequently, the CSP shall scale up (or scale down) the resource requirements (compute, memory, storage, bandwidth etc.) based on the growth in the user compute load / data load / bandwidth load (during peak and non-peak periods / year- on-year increase) to support the scalability and performance requirements of the solution and meet the SLAs. There should not be any constraints on the services.
- There should be sufficient headroom (at an overall level in the compute, network and storage capacity offered) available for near real time provisioning (as per the SLA Meity) during any unanticipated spikes in the user load.
- The scaling up / scaling down (beyond the auto-scaling limits or whenever the auto-scaling limits need to be changed) has to be carried out with prior approval by the department.
- The CSP shall provide the necessary details including the sizing calculations, assumptions, current workloads & utilizations, expected growth / demand and any other details justifying the request to scale up or scale down.
- For any changes to the underlying cloud infrastructure, software, etc. under the scope of the CSP, department shall get alerts / notifications from the CSP, both as advance alerts and post implementation alerts.

3.1.5 Ownership of Data / VMs/ Software

- Department shall retain ownership of all data & applications hosted on CSP's infrastructure and maintains the right to request (or should be able to retrieve) full copies of these at any time (without additional charges).
- Department retains ownership of all virtual machines, templates, clones, and scripts/applications created for the department's application. Department retains the right to request (or should be able to retrieve) full copies of these virtual machines at any time (without additional charges).
- Department retains ownership of loaded software installed on virtual machines and any application or product that is deployed by department on the Cloud Infrastructure.

3.1.6 Compliance

- CSP shall adhere to the standards published (or to be published) by department or any standards body setup / recognized by Government of India and notified to the CSP by department as a mandatory standard.
  The CSP's cloud service offerings shall always remain empaneled / complied with the MeitY guidelines & standards. CSP shall be responsible for the costs associated with implementing, assessing, documenting and maintaining such Empanelment/Compliances.
- CSP shall always remain adhered to the prevailing guidelines issued by MeitY,RBI, CERT-In etc. from time to time.

3.1.7 Documentation

- CSP shall create and maintain all the necessary technical documentation, design documents, standard operating procedures, configurations required to continued operations and maintenance of cloud services.
- The documents which hold critical information, process, policies shall have to be approved by department before release.
- The CSP shall develop, maintain, update following documents as per department requirements:
- Details of inventory for Compute, Storage, Network, Security elements.
- Details of the management, monitoring and helpdesk tools
- The WAN connectivity plan
- Escalation matrix.
- Other details as desired by the department

3.2 Project Requirements

Cloud Service Provider (CSP) shall fulfil the project requirements presented in the subsequent sections.

Business Requirements

B1	Cloud Platform/Infrastructure/Solution shall migrate and host all MITL applications, including e-gov & ERP, e-LMS, GIS dashboard, Electricity Procurement application, Building Plan Approval application, Utility Billing portal and Websites and any other project application as finalised by the Client.
B2	Cloud solution shall have the capability of handling enterprise workloads with auto-scaling features.
B3	The proposed application cloud environment should provide flexibility to scale the environment vertically and horizontally: • Vertically: Upscale/downscale the solution to higher configuration Virtual Machines (i.e. VMs with different combinations of CPU and Memory); and • Horizontally: Add more Virtual Machines of the same configuration to a load balanced pool.
B4	Cloud solution shall be fully secure with no scope of data breach/leaks/thefts/data mining/privacy breach etc.
B5	Cloud solution shall have the characteristics such as rapid elasticity and ability to handle hardware failures without downtime.
B6	Cloud solution shall have extremely high availability of the Compute / Virtual Machines and storage volumes.
B7	In case of failure, cloud solution shall have automated processes which shall move customer data traffic away from the affected area.
B8	Cloud solution shall be complied with ITIL (Information technology Infrastructure library) standards.

FR 1Functional Requirements

CLOUD HOSTING REQUIREMENTS	
It shall provide tools or capabilities that enable users to unilaterally provision / order, manage, and use the Cloud solution with below minimum features.	
FR 1.1	The bidder shall offer Infrastructure as a Service (IaaS) / Platform as a Service (PaaS) / Software as a Service (SaaS) based solution or a combination of the same, as per the bidder's solution.
FR 1.2	The solution shall have the ability of Auto-scaling (Vertical and Horizontal), Scaling up / down on demand.
FR 1.3	It shall have self-service provisioning, where there is near-zero dependency on the CSP and CSP can configure, implement, auto-scale and manage the environment without any human intervention from the CSP.
FR 1.4	It shall have agility with the functionality of software defined configurations to add / remove capacity.
FR 1.5	CSP shall have the overall responsibility the environment and has the ability to log, monitor, and audit the traffic and usage.
FR 1.6	The solution shall have security features out of the box.
FR 1.7	Complete visibility & control of the environment shall be available with the Client – cloud governance capabilities.
FR 1.8	Solution shall provide reporting capabilities (e.g., personal health dashboard, security logs, audit reports) to the Client on the portal with a historical data of minimum period of two weeks.
FR 1.9	User / Admin Portal (User Profile Management, Trouble Management).
FR 1.10	Cloud solution shall be accessible via both Internet and MPLS/VPN
CLOUD INFRASTRUCTURE	
FR 1.11	DC Cloud Infrastructure facilities shall have routers, firewalls, LAN, WAN, internet access, and hosting centres, backup, operations management, and data management capabilities.
FR 1.12	DC Cloud Infrastructure facilities shall have security and data privacy capabilities which include but not limited to data and network security including Anti-Virus, Virtual Firewall, Web Application Firewall, Intrusion Prevention System, Intrusion Detection System, Anti-DDOS, DDOS Protection, Access and Rights Management, Web Application Filter, SIEM etc.
FR 1.13	The data centres must have assured protection with security built at multiple levels and 24x7 monitoring by provisioning physical security, biometric identification and close circuit monitoring.
FR 1.14	Reports of periodic third-party inspections/audits and the certifications shall be available online or shared on demand for scrutiny.
FR 1.15	DC facility shall support multiple of databases such as – PostgreSQL, MySQL, Oracle, Hana and MS SQL Server etc.
FR 1.16	DC facility shall be capable of offering following platform services: • Analytics Services;

	• IoT and Big Data Services; • Mobile Services.
Disaster Recovery Centre (DRC) / Secondary DC	
DRC / Secondary DC as a Service may be opted in future as per Client discretion. Below functionalities shall be complied by the CSP in case DRC / Secondary DC as a Service is utilised.	
FR 1.17	Cloud solution shall be offered from physically apart data centres (Primary and Secondary Data Centre / Disaster Recovery Centre (DRC) in India to provide business continuity with no interruptions in case of any disruptions/disaster to one of the data centre facility.
FR 1.18	A cloud solution provider is required to suggest most cost-effective architecture to meet the Data Centre and disaster recovery requirements as presented in the RFP. The proposed architecture can be hosted in Active-Active mode or Active Passive mode based on the recommendation of cloud service provider architecture. The architecture shall support resource optimisation and load balancing.
FR 1.19	In case of failure of the data centre, operations shall be resumed from the Secondary Data Centre / Disaster Recovery Centre (DRC).
FR 1.20	CSP shall adhere to the RPO and RTO requirements
FR 1.21	During the change from DC to secondary DC / DRC or vice-versa (regular planned changes) there should not be any data loss.
FR 1.22	Secondary DC / DRC Cloud Infrastructure shall have security and data privacy capabilities which include but not limited to data and network security including Anti-Virus, Virtual Firewall, Web Application Firewall, Intrusion Prevention System, Intrusion Detection System, Anti-DDOS, DDOS Protection, Access and Rights Management, Web Application Filter, SIEM etc..
FR 1.23	Secondary DC / DRC facilities shall have security and data privacy capabilities which include but not limited to data and network security including Anti-Virus, Virtual Firewall, Single Sign-on, One Time Password, Multi Factor Authentication, SSL, DDOS Protection, Rights Management, Web Application Filter, etc.
FR 1.24	Secondary DC / DRC must have assured protection with security built at multiple levels and 24x7 monitoring by provisioning physical security, biometric identification and close circuit monitoring.
FR 1.25	Reports of periodic third-party inspections/audits and the certifications shall be available online or shared on demand for scrutiny.
FR 1.26	Secondary DC / DRC facility shall support multiple of databases such as – PostgreSQL, MySQL, Oracle, Hana and MS SQL Server etc.
FR 1.27	Secondary DC / DRC facility shall be capable of offering following platform services: • Analytics Services; IoT and Big Data Services; Mobile Services.
Cloud Governance Capabilities	
Solution shall have an audit and compliance features which enables the Client agency to monitor the provisioned resources, performance, resource utilization, and security compliance. It shall have the following functionalities:	
FR 1.28	Monitoring of cloud resources with alerts to Client 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.
FR 1.29	Automated security assessment services to improve security and compliance of applications deployed on cloud by automatically assessing applications for vulnerabilities or deviations from best practices.
FR 1.30	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.
FR 1.31	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.
FR 1.32	Event-based alerts, to provide proactive notifications of scheduled activities, such as any changes to the infrastructure powering the cloud resources.
FR 1.33	Capture logs of all user activity within an account. This is required to enable security analysis, resource change tracking, and compliance auditing.
FR 1.34	Ability to discover all provisioned resources and view each of the configuration. Notifications shall be triggered each time a configuration changes, and agencies shall be given the ability to dig into the configuration history to perform incident analysis.
FR 1.35	Continuous monitoring and optimization of auto-scaling rules and limits.
FR 1.36	Optimize overall cost of resources require to run overall operations of the Client.
FR 1.37	Cloud infrastructure should not allow any data mining, data theft, data breach violations of any type.
Track Resource Inventory and Changes	
FR 1.38	Resource inventory, configuration history & change notifications functionalities shall be provided.
FR 1.39	Guidelines for provisioning, configuring and continuously monitoring compliance shall be provided.
FR 1.40	Solution shall automatically records a resource's configuration when it changes.
FR 1.41	Solution shall examine the configuration of resources at any single point in the past.
FR 1.42	Client shall receive notification of any configuration change.
Personalized Dashboard	
FR 1.43	Dashboards shall provide a personalized view of service health, consumption and usage.
FR 1.44	Dashboards shall provide proactive notifications.
FR 1.45	Dashboards shall have the capability of detailed troubleshooting guidance.
FR 1.46	Dashboards shall have the capability of integration and automation.

Technical Requirements

General

The cloud solution shall provide flexibility of hosting the applications on VMs of varying configuration scales.

Cloud solution shall have demonstrable capability to provide a market place where Client can pick first party and third party applications for ready deployment. Applications for Firewall, Email Service, Logging and Monitoring service, translation service, document signing service etc. shall be available on an additional Pay-per-use model.

Cloud solution shall have a Cloud Management interface which shall have the ability to unilaterally provision and de-provision the specific IaaS/PaaS/Saas services contemplated by the project via Web Portal and Web Services Application Programming Interface ("API"). All the communication for these purposes shall be secured at transport level using SSL / TLS / SSH.

Cloud solution shall have "Auto Scale" capability enabling provision of additional resources based on the seasonal peak loads.

Hosting solution shall have the ability to provision virtual machines, storage and bandwidth dynamically (or on-demand), on a self-service mode or as requested.

The service shall offer a secure Web administration interface, which shall provide to remotely administer the virtual instances: RDP for Windows instances and SSH for Linux instances.

The service shall allow users to copy or clone virtual machines images for archiving, troubleshooting, and testing.

The service shall provide the ability to provision Block Storage capabilities for the virtual machine instances. These storages can be dynamically scalable on-demand and Virtual Machine instances shall be able to mount it as OS drives.

Cloud solution shall provide interoperability support with regards to available APIs, data portability etc. for Client to utilize in case of Change of cloud service provider, migration back to in-house infrastructure, burst to a different cloud service provider for a short duration or availing backup or DR services from a different service provider.

The public facing services shall be deployed in a zone (DMZ) different from the application services. The Database nodes (RDBMS) shall be in a separate subnet with higher security layer. The UAT and training portals on the cloud shall be separate from the production portal in a different subnet than the production environment and setup such that users of the environments are in separate networks.

Cloud service shall have suitable security and networking solutions

Cloud service shall provide real-time analytics and enable trend identifications on the usage.

Integration

Cloud solution shall provide an API for each of the required services that enables the development of complex automation solution for resource provisioning, configuration and de-provisioning.

The APIs shall be based on open interoperable standard such as REST.

Cloud solution shall provide APIs to consume the services and complete documentation for all the APIs it offers.

Cloud solution shall provide API management features as a native capability. It shall provide real-time analytics and enable trend identifications on the usage of the published API's.

Cloud solution platform shall support multiple operating systems, at a minimum Windows, Red Hat Linux, SuSe, Oracle EL, etc.

Cloud solution shall support SDKs for this APIs for platforms like Microsoft .net, Java/JavaScript, Python, PHP or Ruby.

Capability shall be provided where all APIs are managed from a single place.

Network Services

Cloud solution shall provide IP addressing that shall support: IPv4, IPv6, DHCP, IP address and port assignment on external (public) interfaces, dedicated VPN connectivity and the ability to map Project DNS domains to CSP services addresses enabling services, sites and applications operating in the CSP infrastructure to be viewed as URLs.

Cloud service shall provide a traffic management mechanism to implement availability based load balancing for virtual Machine Instances.

Cloud solution shall provide virtual private network (VPN) connectivity from cloud environment in both Site-to-Site and Point-to-Site configurations.

Cloud solution shall provide an option of extending an MPLS to cloud.

Cloud service provider's infrastructure shall be protected against DDoS.

Cloud solution shall provide virtual network isolation capabilities among the virtual machines and must support the use of private virtual networks.

Cloud service provider shall have multiple ISPs providing Internet connectivity to their data centre / network.

Cloud service shall provide connectivity with options to leverage carrier provided MPLS and shall be backed by SLA.

Direct peering with large TSPs in India for speedy and efficient delivery of content to all users accessing the service from various devices on various network service providers.

The proposed cloud platform shall have ability to deploy VMs in multiple security zones, as required for the project, defined by network isolation layers in the Client's local network topology.

The cloud solution shall be able to monitor VM up/down status and resource utilization such as RAM, CPU, Disk, IOPS and network

Provide hardware or software based virtual load balancer Services (VLBS) through a secure, hardened, redundant CSP Managed Virtual Load Balancer platform.

Security, Privacy and Compliance Requirement

Following security features shall be provided as part of the Cloud solution:

1. Availability of global third-party certifications: Cloud Services shall be certified (by a third party) for ISO 9001, ISO 27001, ISO 20000
2. Identity and Access Management (IAM): that allows controlling of level of access to the users to the CSPs infrastructure services. With IAM, each user shall have unique

security credentials, eliminating the need for shared passwords or keys and allowing the security best practices of role separation and least privilege;;

3. Cloud solution shall provide Directory service as a cloud service backed by SLA. The Identity service shall allow single sign-on (SSO);
4. Secure Access – Client access points, also called API endpoints, shall allow secure HTTP access (HTTPS) so that the Agencies shall establish secure communication sessions with Cloud services using Secure Sockets Layer (SSL)/Transport Layer Security (TLS) (Latest version).

Solution shall have capability of Role Based Access Control to segregate users based on their roles and privileges.

Cloud solution shall provide flexibility to choose various firewall and router solutions from the industry leading vendors or as requested by Client.

Cloud solution shall manage the underlying hardware infrastructure and virtualization layer following the appropriate patch management and technology refresh cycles.

Cloud solution shall support Network and security with virtual firewall and virtual load balancer integration for auto-scale functions.

Following security solutions shall be procured and implemented by CSP via third party:

1. Anti-Virus for the virtual machines;
2. Host Intrusion Detection System;
3. Web Application Firewall to help protect web applications from common web attacks such as SQL injection or cross-site scripting;
4. SIEM (Security Incident and Event Management) to monitor the security incidents.

Cloud solution shall be fully secure and should not allow any data privacy breach, security breach, data mining, data corruption of any type.

Additional Features

Following components shall be part of the cloud solution and shall be quoted as part of the financial Proposal:

Operating System, Antivirus/Antispam/Antimalware, Patch Management Tools for non-Windows/Linux OSs.

Provide the user administration / portal of cloud services to have visibility into the dashboard, SLAs, management reports, etc.

Additional Third Party Firewalls.

Management, Monitoring and Audit: Security Information and Event Management tools, Performance Monitoring Tools, Patch/Update Management Tools for OS, DB.

VPN: VPN server / gateway for providing VPN connectivity to some set of users.

Any additional tools required to run the cloud application in a secure manner shall be proposed.

The system shall be able to restore from the backup whenever required.

Configure, schedule, monitor and manage backups of all the data including but not limited to files, images and databases.

4 Cloud Compute Requirement

4.1 Provisioning of Virtual Machine (VM's)

- Virtual Machines shall be required to run the variety of workloads such as compute-intensive workload, memory-intensive workload, general-purpose workload, etc. The CSP shall deploy VMs on Server-Hardware having 1:2 Physical Core to vCPU ratio.
- CPU (Central Processing Unit) shall be provided with a minimum equivalent processor speed of 2.4GHz. The CPU shall support 64-bit operations.
- Department reserves the right to get the landscape audited by OEM, if deemed necessary.
- The virtual machine shall be capable of running different operating systems (Linux, Windows etc.) with any of their variants/ versions.
- Monitor VM up/down status and resource utilization such as RAM, CPU, Disk, IOPS and network.
- Department retains ownership of all virtual machines, templates, clones, and scripts/applications created for the department's application.
- Provide facility to configure virtual machine of required vCPU, RAM and Disk.
- Provide facility to use different types of disk like SAS, SSD based on type of application.

4.2 Administration, Configuration & Training

- Upon deployment of virtual machines, the CSP has to assume full administrator access and is responsible for performing additional configuration, security hardening, vulnerability scanning, application installation, troubleshooting, hardening, patch/ upgrades deployment, BIOS & firmware upgrade as and when required.
- CSP shall ensure Preparation / Updation of the new and existing Standard Operating Procedure (SOP) documents on servers & applications deployment and hardening.
- CSP shall ensure Patching of VMs on the next available patch management via change window and / or provide self-service tools to patch VMs.
- The CSP shall be setting up and configuring servers and applications as per configuration documents/ guidelines provided by department.
- The CSP shall do Installation/ re-installation of the server operating systems and operating system utilities in the VMs.
- CSP shall make provision to Monitor VM up/down status and resource utilization such as RAM, CPU, Disk, IOPS and network
- CSP shall monitor availability of the servers, CSP-supplied operating system & system software, and CSP's network.
- CSP shall ensure that VMs receive OS patching, health checking, Systematic Attack Detection, and backup functions.
- Monitor VM up/down status and resource utilization such as RAM, CPU, Disk, IOPS and network.
- CSP shall arrange training for 5 nos. department personnel on proposed cloud platform from OEM with certification.

4.3 Cloud Security Administrator

The CSP shall provide 24x7x365 managed services for the entire security stack protecting the department environment. CSP shall be responsible for managing configuration and patch management, vulnerability scanning, protecting data in transit and at rest, managing credentials, identity, and access management etc. The activities include:

- Appropriately configure the security groups in accordance with the Security policies

- Regularly review the security group configuration and instance assignment in order to maintain a secure baseline.
- Secure and appropriately segregate / isolate data traffic/application by functionality using DMZs, subnets etc.
- Ensure that the cloud infrastructure and all systems hosted on it, respectively, are properly monitored for unauthorized activity
- Conducting regular vulnerability scanning and penetration testing of the systems, as mandated by their Government Agency's policies
- Review the audit logs to identify any unauthorized access to the government agency's systems.
- The protection from unauthorized usage, detection of intrusions, reporting as required and proactive prevention actions are to be provided by CSP.
- Service Component Administration
- User and Password Control
- Check and maintain access control
- Routine connection tests
- Change & Configuration Management
- IP / Port / Zone Configuration
- Firewall policy / IPsec VPN / SSL VPN configuration
- NAT / PAT configuration
- Multicast configuration
- Antivirus / IPS Signature update, when released by vendor
- Fault Management
- Response to alerts generated by systems or problems reported.
- Troubleshooting, root cause analysis (RCA) and identification of problem area
- Resolution of problems through configuration changes/ re-installations / replacements
- Escalate hardware failures to hardware vendor
- Assist hardware vendor to Identify problem area (by log collection & reboot)
- Log Storage: Store critical logs in shared Syslog server for retention period of 90 days
- Configuration backup: Take incremental configuration backup daily for retention period of 90 days and Restoration of configuration when required.
- Trouble ticket logging, update, and closure
- Managing configuration and security of Demilitarized Zone (DMZ) Alert / advise department about any possible attack / hacking of services, unauthorized access / attempt by internal or external persons etc.
- Incident Response - The CSP should have policies and procedures in place for timely detection of vulnerabilities within organizationally owned or managed applications, infrastructure network and system components (e.g., network vulnerability assessment, penetration testing) to ensure the efficiency of implemented security controls. The CSP must also have policies and procedures in place to ensure timely and thorough incident management, as per established IT service management policies and procedures. The Solution shall be complied with ITIL (Information technology Infrastructure library) standards.

4.4 Cloud Portal

- The cloud virtual machine created by portal should be have at-least two virtual NIC cards. One NIC card should be used for internet traffic while other should be used for internal service traffic.
- Cloud service should enable to provision cloud resources through self service provisioning interface.
- Should be able to create, delete, shutdown, reboot virtual machines from Cloud portal.
- Should be able to set threshold of cloud resources of all types of scalability.
- Cloud System should support provisioning from self-Cloud Orchestration System to add more storage as and when require by VM.
- Cloud System should give provision to attached new block disk to any cloud VM from self service portal.
- Cloud System should have provision to ensure that cloud virtual machine is into separatenetwork tenant and virtual LAN.
- Cloud System must ensure that cloud virtual machines are having private IP network assigned to cloud VM
- Cloud System must ensure that cloud virtual machines are having private IP network assigned to cloud VM.
- Should support use of appropriate load balancers for network request distribution across
- multiple cloud VMs.
- Cloud Orchestration System should provide network information of cloud virtual resources.
- The Admin should be able to define Access Control to Permit or Deny operation per Group or per User.
- Should have provision to define Workflow to Escalate Permission to Group Admins or System Admins.
- Cloud System should give provision to make clone of cloud virtual machine from Cloud Orchestration System.
- Cloud System should have provision to migration of virtual machine from one hypervisor platform to another hypervisor platform through its UI.
- Cloud System cloud shall continuously monitor utilization across Virtual Machines and shall intelligently allocate available resources among the Virtual Machines.
- The Cloud System solution shall be able to dynamically allocate and balance computing capacity across collections of hardware resources of one physical box aggregated into one nified resource pool.
- The solution shall provide near zero downtime host patching with maintenance mode to move running workloads to other hosts on the platform with a consistent audit trail of the patching process.
- Cloud System should give provision to monitor the network traffic of cloud virtual machine.
- Cloud System should offer provision to analyse of amount of data transferred of each cloud virtual machine.
- Cloud System must offer provision to monitor uptime of each cloud virtual machine.
- Cloud System must make provision of resource utilization i.e. CPU graphs of each cloud virtual machine.
- Cloud System must give provision to monitor the load of Linux/Windows servers and set threshold for alerts.
- Cloud System must ensure that there should be historical data of minimum 6 months for resource utilization in order to resolve any billing disputes if any.

4.5 Cloud Portal Service Provisioning

- Should be able to predict his billing of resources before provisioning any cloud resources.
- Department should be able to set threshold of cloud resources of all types of scalability.
- Should be able to set minimum and maximum number of virtual machines which will be automatically provisioned as part of horizontal scaling to handle spike in load.

5 Application Performance Monitoring (APM)

The Application Performance Monitoring (APM) solution shall be supplied on a perpetual license basis in the name of MITL, for the number of instances/units specified in the Bill of Material. The perpetual license, together with all necessary entitlements, shall survive the expiry or termination of this contract and shall remain the property of MITL. The CSP shall provide OEM support, software updates, maintenance patches and version upgrades for the APM solution for the initial contract period at no additional cost. Support, updates and maintenance during any extension period shall be chargeable as separately agreed under the Extension of Contract and Payment Terms clauses. On completion of the contract, the CSP shall hand over the perpetual licenses, current configuration and administrative credentials of the APM solution to MITL or its designated agency as part of exit management.

Application Performance Monitoring (APM) — Functional Compliance		
Sr. No	**APM Functional Requirement**	**Compliance (Y/N)**
1	The solution shall provide proprietary instrumentation agents for comprehensive application performance monitoring across supported environments.	
2	The solution shall support deployment in on-premises, sovereign, and fully air-gapped environments without dependency on external cloud services.	
3	The solution shall provide monitoring and performance visibility for High-Performance Computing (HPC) and GPU-based workloads.	
4	The solution shall include an in-house AI/ML-driven anomaly detection engine capable of identifying performance deviations and operational abnormalities.	
5	The solution shall provide full-stack distributed tracing to enable end-to-end transaction visibility across applications, services, and infrastructure layers.	
6	The solution shall support Real User Monitoring (RUM) in on-premises environments to capture actual user experience metrics and application behavior.	
7	The solution shall provide deployment impact analysis capabilities to assess the effect of application releases, patches, and configuration changes on performance.	
8	The solution shall generate compliance and reporting outputs aligned with CERT-In and RBI monitoring and audit requirements.	
9	The solution shall support topology-aware alerting with contextual correlation across application, infrastructure, and dependency layers.	
10	The solution shall offer a unified licensing model without host-based, node-based, or per-server licensing restrictions.	

6 Database Activity Monitoring (DAM)

The Database Activity Monitoring (DAM) solution shall be supplied on a perpetual licence basis in the name of MITL, for the number of instances/units specified in the Bill of Material. The perpetual licence, together with all necessary entitlements, shall survive the expiry or termination of this contract and shall remain the property of MITL. The CSP shall provide OEM support, software updates, maintenance patches and version upgrades for the DAM solution for the initial contract period at no additional cost. Support, updates and maintenance during any extension period shall be chargeable as separately agreed under the Extension of Contract and Payment Terms clauses. On completion of the contract, the CSP shall hand over the perpetual licences, current configuration and administrative credentials of the DAM solution to MITL or its designated agency as part of exit management.

Sr. No	DAM Functional Requirement	Compliance (Y/N)
1	The solution shall provide a proprietary Database Activity Monitoring (DAM) engine for monitoring and securing database environments.	
2	The solution shall support deployment in sovereign, on-premises, and fully air-gapped environments.	
4	The solution shall provide active real-time blocking capabilities to prevent unauthorized or suspicious database activities.	
5	The solution shall support native connectors and integrations for Indian banking core systems and related enterprise applications.	
6	The solution shall provide broad database platform coverage across heterogeneous database environments.	
7	The solution shall generate audit reports aligned with RBI, SEBI, and CERT-In compliance and regulatory requirements.	
8	The solution shall support Privileged User Behaviour Analytics (PUBA) for monitoring, profiling, and detecting anomalous privileged user activities.	
9	The solution shall provide in-premises data discovery and classification capabilities to identify, categorize, and protect sensitive information.	
10	The solution shall maintain immutable audit trails with legal admissibility to support forensic investigations and compliance requirements.	
11	The solution shall support zero-latency out-of-band monitoring without impacting database performance or production workloads.	
12	The solution shall provide bidirectional SIEM integration along with native incident management and workflow capabilities.	
13	The solution shall support secure multi-tenant isolation suitable for Cloud Service Providers (CSPs), cloud environments, and shared infrastructure deployments.	

7 PIM / PAM Services

Sr.	Description	Compliance Y/N
1	The proposed solution should be able to seamlessly integrate with the existing solution and support all the Operating Systems including but not limited to Windows, Unix, Linux, Solaris, etc.	
2	The proposed solution should be able to integrate with applications including but not limited to web applications, thick clients, etc.	
3	The proposed solution should be able to int egrate with other security solution including but not limited to Firewall, IPS/IDS, etc.	
4	The proposed solutions should be able to integrate with network devices including but not limited to switches, routers, etc.	
5	The proposed solutions should be able to integrate with databases including but not limited to MySQL, Oracle, HBase, MSSQL, etc.	
6	The proposed solution should be agentless.	
7	The solution should be able to integrate with the proposed enterprise authentication methods –Active Directory, LDAP.	
8	The solutions should provide a single platform to access all the integrated devices and solutions	
9	The solution should have the capability to monitor session activities in real time and should maintain audit logs of the same	
10	The solution must provide two factor authentication mechanism	
11	The solution should be capable of providing real time dashboard and	
12	The solution should maintain audit trails for all administrative and user access and activities	
13	The solution should be common criteria compliant	
14	The solution should have the capability to track privileged identities or privileged account activities distinctively	
15	The solution should contain a password vault which should enable an administrator to define different password formation rules for target accounts on different target systems and supports the full character set including special characters that can be used for passwords on each target system.	
16	The solution should set unique random value anytime a password is changed.	
17	The solutions should provide a single console for all administrative tasks	
18	The solution should be capable of user and group level access with multi-level administrative access	
19	The solution should be able to restrict usage of critical commands over an SSH console-based session on any combination of target account, group or target system and end-user.	

Sr.	Description	Compliance Y/N
20	The solution should restrict privileged activities on a windows server (e.g. host to host jumps, Power shell, cmd/telnet access, application access, tab restrictions etc.) from session initiated with PIM.	
21	The solution should be able to restrict usage of critical commands and/or tables for database access through SSH, Database Client utilities (TOAD, SQL developer) on any combination of target account, group or target system and end-user.	
22	The solution should have maker-checker control built-in for all administrative functions (password changes, system configuration etc.).	
23	The solution can restrict target -account-specific entitlements of end users individually or by group or role.	
24	The solution should log all the admin activity and that should be monitored.	
25	The solution can restrict end-user entitlements to target accounts by days and times of day.	
26	The solution must support parallel execution of password resets for multiple concurrent requests.	
27	The solution should provide fully automatic failover from a single active instance to a backup/standby instance with a fully replicated repository.	
28	The solution should be able to integrate with the ticketing tools for Incident/Change management.	
29	The solution should automatically archive session recording data to external storage/ media based on time and available space.	
30	The solution provides the capability to enable end users to retrieve (or reset) a target -system password only after electronic approval by a designated approver. Approval criteria can be based on any combination of target account, group or targ et system and end-user identity, group or role, as well as contextual information such as day of the week or time of day.	
31	The solution should be able to perform auto discovery of privileged accounts on target systems and able to perform two-way reconciliation.	
32	The solution should be scalable in terms of the system administrators, target systems and the concurrent session.	
33	The tool must have the required APIs for integration with GRC, SIEM tools etc. or linkage of change & release tickets while raising access ticket request within the tool by the requestor.	
34	The solution should be scalable in terms of the system administrators, target systems and the concurrent session.	
35	ii. The solution should integrate with the solutions proposed as a part of the Data Centre Security like SIEM, DAM, Vulnerability Management etc.	
36	The solution should integrate with the proposed Enterprise Management Solution.	

8 Email Services (Email as a Service)

#	Functional Requirement	Compliance (Yes/No)
1	Enterprise-grade business email service for the number of user IDs specified in the Bill of Material, provisioned on the Department's official domain, with the ability to add or remove user IDs on demand with pro-rata billing.	
2	Mailbox size of minimum 50 GB per user ID, with configurable per-user quota management.	
3	Secure web-based mail client (webmail) accessible over HTTPS, along with support for standard mail protocols (SMTP, IMAP4, POP3) and mobile device synchronization (Exchange ActiveSync or equivalent open protocol) for iOS and Android devices.	
4	Integrated calendaring, contacts, tasks, global address list, distribution lists, and shared/group mailboxes.	
5	Web-based administration console for complete user-ID lifecycle management (creation, suspension, deletion, password policy, quota, delegation) with role-based administrative access.	
6	Directory integration (Active Directory/LDAP) and support for SSO using SAML 2.0/OAuth 2.0; Multi-Factor Authentication (MFA) for webmail and administrative access.	
7	Built-in anti-spam, anti-phishing and anti-malware scanning of all inbound and outbound mail, including attachment and URL protection, with quarantine management.	
8	Enforcement of SPF, DKIM and DMARC for the Department's domain; TLS 1.2 or higher for all mail in transit; encryption of mailbox data at rest.	
9	Email archival/journaling with configurable retention policies and search/eDiscovery capability for compliance and audit requirements.	
10	Data Loss Prevention (DLP) policy support for outbound email (keyword, pattern and attachment-based rules).	

11	Backup and restore of mailboxes, including deleted-item and deleted-mailbox recovery with configurable retention period.	
12	Audit logging of administrative and user-level activities, with logs retained for a minimum of 180 days within India and capable of integration with the SIEM service under this contract.	
13	Migration of existing mailboxes and data (if any) from the incumbent email environment at no additional cost.	
14	Service availability of minimum 99.9%, measured quarterly, governed under the SLA and penalty framework defined in Section 11 of this RFP.	

9 CSP SCOPE OF WORK

The Project requires turnkey services wherein the CSP shall broadly cover the following main scope of services:

5. Installation and coordination with MSI;
6. Migration & Testing;
7. Commissioning and Operational Acceptance;
8. Operations, Management and Support of cloud infrastructure.

The subsequent sections detail out the scope with respect to execution of this Project. The CSP shall note that the activities defined within scope of services mentioned are indicative and may not be exhaustive. CSP is expected to perform independent analysis of any additional work that may be required to be carried out to fulfil the requirements as mentioned in this bid document and factor the same in its response.

Below are mentioned the scope of services, provided in phases, which have to be carried out as part of the Project:

9. Project Management Phase;
10. Implementation of Cloud Infrastructure Phase including Migration of existing MITL Applications
11. Stabilization and Operational Acceptance of Cloud Infrastructure Phase;
12. Operations and Maintenance Support of Cloud Infrastructure Phase.

9.1 Project Management Phase

CSP shall be responsible for end to end project management for the implementation and support of cloud and Cloud services provided for MITL. CSP shall deploy Project Manager and a Project Coordinator for the purpose of Project Management.

The Project Manager shall be the single point of contact that shall assume overall responsibility of the Project and ensure end to end working of the Project. He shall function as the primary channel of communication for all Client requirements to the implementation team. In case of any absence of the project manager (sickness or vacation), the CSP shall ensure that an alternate project manager (as approved by the client or its representative) shall be provided during the absence period.

CSP shall be responsible for preparing a master schedule of work which shall highlight implementation plan for all the Project milestones. The schedule shall also show Client and any third-party responsibilities along with the activities in the timeline. CSP shall attend meetings with the Client (and/or its representative) whenever required.

CSP shall also be responsible for effective risk and issue management and escalation procedures along with matrix as part of project management. CSP shall identify, analyse, and evaluate the project risks and shall develop cost effective strategies and action plan for mitigation of risks. As part of the Project CSP shall monitor, report and update risk management plans and shall be discussed during project meetings.

CSP shall prepare minutes of every meeting which takes place and submit to Client or its representative for tracking of the Project. CSP shall propose a suitable progress reporting mechanism for the project duration.

All the tools required by CSP for project management, configuration management, issue and risk management, escalation procedure and matrix document repository etc. shall be factored in the proposal submitted by CSP.

Based on progress reports, CSP shall also accordingly update the master schedule of work on a continuous basis during the period of the contract.

The success of the project depends on the proper project planning and management. At the onset, the Bidder shall plan the project implementation in great details and should provide a micro level view of the tasks and activities required to be undertaken in consultation with department. An indicative list of planning related documentation that the Bidder should make at the onset is as follows:

- Project Schedule: A detailed week-wise timeline indicating various activities to be performed along with completion dates and resources required for the same
- Manpower Deployment List: A list needs to be provided with resources who will be deployed on the project along with the roles and responsibilities of each resource.
- Resource Deployment List: List and number of all cloud-based resources (including but not limited to servers (VMs), storage, network components and software components) other than manpower that may be required.
- Communication Plan: Detailed communication plan indicating what form of communication will be utilized for what kinds of meeting along with recipients and frequency.
- Migration Plan: The Bidder will be required to submit a migration plan to department for migrating the application on its Cloud. Necessary support will be provided by the application vendor of department.
- Progress Monitoring Plan and Reporting Plan: Detailed Daily, Weekly, Monthly Progress Report formats along with issue escalation format. The format will be approved by department to the successful bidder before start of the project.
- Standard Operating Procedures: Detailed procedures for operating and monitoring the Cloud site.
- Risk Mitigation Plan: List of all possible risks and methods to mitigate them.
- Escalation Matrix & Incident Management: A detailed list of key contact persons with contact details with escalation hierarchy for resolution of issues and problems. This has to be via an Incident Management system.

- Training Strategy: The training strategy should be designed to provide training to the IT technical team personnel identified by department. Department will measure the effectiveness after the completion of the training through training feedback forms. A formal training plan with relevant course material is required as part of the training session.

9.2 Implementation of Cloud Infrastructure Phase, including Migration of Existing MITL applications

As part of the implementation of cloud infrastructure phase, CSP scope of services shall be as following:

9.2.1 Data Centre

- Provide required IT infrastructure as IaaS for hosting Client's applications.
- Provide the required compute infrastructure (server/virtual machines), storage and services for hosting Client applications as per application requirements.
- Support e-LMS SI and MSI in the migration of the existing and operational system from the existing infrastructure to the new infrastructure with below activities

A. Migration Planning: Comprehensive planning for migration of the application suite and data to the cloud, developing the migration roadmap, and identifying the constraints and inhibitors to cloud migration. The migration plan shall also include a plan for the co-existence of existing-cloud and new-cloud architectures during and after migration and test plans for verifying successful migration. Also, this exercise shall support working with MSI and Client for optimising the architecture and hosting requirements. Migration Plan shall also include a downtime plan, if required, which may be required as part of the migration of applications from the existing cloud infrastructure to the proposed cloud Infrastructure/Platform. Any downtime required during migration has to be approved by MITL.

B. The migration shall also include the migration of underlying data & files from the current database(s) / storage into the database(s) / storage on the cloud.

C. Provision necessary compute & storage infrastructure on the cloud to host the Application Suite that meets or exceeds the day-1 minimum capacity.

D. Set up of Development, Quality, and Production Environments by provisioning the necessary compute & storage infrastructure on the cloud, along with the underlying software licenses to host the Application Suite.

E. Configuring external connections to the hosted infrastructure is required to upload database backups and virtual machine (VM) images to the hosting environment.

F. Migration of all applications from the existing environment to the proposed Cloud Platform, along with end-to-end testing.

G. Any downtime required during the Migration process has to be minimal so as it does not to impact the business operations of MITL.

1. CSP shall be responsible for migration and hosting of all existing MITL applications developed by e-LMS SI and MSI, including but not limited to:
2. E-Gov and ERP Applications;
3. E-LMS Application
4. Mobile Applications;
5. Utility Billing application
6. CDCPR and GIS application

7. Electricity procurement application
8. Any other applications commissioned by the Client for meeting their requirements.
9. The application software, the necessary licenses for deploying Client applications ecosystem, comprising of the work streams shall be provided by e-LMS SI for e-LMS system and MSI. PaaS Requirements - While the MSI and e-LMS SI have procured the software licenses, any additional requirements may also be required to be provisioned by the CSP as Platform as a Service (PaaS).
10. The CSP shall ensure through CSP for providing Internet Bandwidth and connectivity at the DC & Secondary DC / DRC, including termination devices, for end users to access Client application from Client premises and from anywhere based on access rights.
11. The CSP shall use the Cloud Services to monitor the service levels and utilizations of the server, storage and other services. Where required, the CSP shall provision additional monitoring tools for measuring the application performance-related service levels. The payments shall be made to the CSP based on the consumption of the Cloud Services.
12. The CSP shall be responsible for ensuring the security of Client applications and infrastructure from any threats and vulnerabilities. The CSP shall address ongoing needs of security management, including, but not limited to, monitoring of various devices/tools such as firewall, intrusion prevention/ detection, content filtering and blocking, virus protection, even logging & correlation and vulnerability protection through implementation of proper patches and rules.
13. The solution needs to provide the ability for Client's IT Administrators to automatically provision the services via a Web Portal (Self-Provisioning), provide metering and billing to provide service assurance for maintenance & operations activities.
14. The CSP shall prepare and submit a project plan with mapping of infrastructure at DC site including following parameters:
15. Server Provisioning
16. Storage Requirements
17. Network interfaces requirement
18. Network throughput requirement
19. Adequate Backup requirement
20. Failover mechanism for replication links
21. On acceptance of project plan by Client the CSP shall implement the cloud solution and offer for testing.
22. While the initial sizing & provisioning of the underlying infrastructure (including the system software and bandwidth) may be carried out for the first year; subsequently, it is expected that the CSP, based on the growth in the user load (peak and non-peak periods; year-on-year increase), shall scale up or scale down the compute, memory, storage, and bandwidth requirements to support the scalability and performance requirements of the solution and meet the SLAs using the auto-scaling features provided by the CSP.

9.2.2 DRC / Secondary DC:

The Cloud Service Provider shall provide the services in accordance with the penalty terms and Service Level Agreement (SLA) Matrix specified in the RFP.

9.3 Stabilization and Operational Acceptance of Cloud Infrastructure Phase

As part of stabilization and operational acceptance of the cloud infrastructure phase, CSP scope of services shall be as following:

1. The CSP shall facilitate Operational Acceptance Tests. Operational acceptance tests shall be performed by Client or its representative. However, CSP shall have to facilitate Operation Acceptance during commissioning of the system, to ascertain whether the system conforms to the scope of services. The CSP shall facilitate the testing of application from the Client users during the Operational Acceptance. Necessary support shall be provided by the application vendor of the Client.
2. Operational Acceptance testing shall be completed after the cloud solution has been provisioned and switchover testing (as applicable) has been completed.
3. For final Operational Acceptance of Cloud Infrastructure, all the Applications migrated, commissioned and hosted on the Cloud Platform shall be monitored for 15 days. Post successful completion and sign-off from MITL for this stabilisation phase, Operational Acceptance shall be provided.
4. CSP shall address any deficiency, if any, reported by the Client or its representative during operational acceptance tests and the Stabilisation Phase. CSP shall address all concerns and make necessary upgrades at no additional cost to the Client.

9.4 Operations and Maintenance Support of Cloud Infrastructure Phase.

As part of operations and support of cloud infrastructure phase, for the infrastructure being provided by CSP, scope of services shall be as following:

9.4.1 Data Centre

1. The CSP shall be responsible for providing 24*7*365 days managed services and support for Client Cloud infrastructure from the date of issuance of operational acceptance by Client till end of the contract which shall be backed by commercial support from CSP. CSP shall provide at least two contact details for helpdesk and centralized email for attending Client requests and complains.
2. CSP shall be responsible for resource management in coordination with MSI as per following:
3. Provide the required compute, memory, and storage required, building the redundancy into the architecture (including storage) and load balancing to meet the service levels;
4. Provide ability to provision virtual machines, and storage dynamically (or on-demand), on a self-service mode or as requested;
5. CSP shall offer fine-grained access controls including, conditions like time of the day, originating IP address, use of SSL certificates, or authentication with a multi-factor authentication device;
6. Patch & Configuration Management
    - User Administration

7. CSP shall implement Identity and Access Management (IAM) that 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;
8. CSP shall be responsible for administration of users, identities and authorizations, properly managing the root account, as well as any Identity and Access Management (IAM) users, groups and roles they associated with the user account;
9. The CSP shall support multiple users with a management portal;
10. The CSP shall provide Billing / Invoice tracking through a web portal aggregated by user application and service at mutually agreed intervals.
11. CSP shall be responsible for security administration. CSP shall:
12. Appropriately configure the security groups in accordance with the Client's networking policies;
13. Regularly review the security group configuration and instance assignment in order to maintain a secure baseline;
14. Secure and appropriately segregate / isolate data traffic/application by functionality using DMZs, subnets etc.;
15. Ensure that the cloud infrastructure and all systems hosted on it, respectively, are properly monitored for unauthorized activity;
16. Implement anti-malware and host-based intrusion detection systems on instances, as well as any required network-based intrusion detection systems in accordance with the Client's policies;
17. Review audit logs to identify any unauthorized access to the cloud infrastructure.
18. Shall provide mechanisms to enable data isolation and privacy in its environment.
19. Conduct regular independent third-party assessments of the CSP's security controls to determine the extent to which security controls are implemented correctly, operating as intended, and producing the desired outcome. CSP shall make these reports available to customers via a secure portal.
20. The CSP shall conduct vulnerability and penetration test (from a third-party testing agency) on the environment provisioned for Client every 6 months and reports shall be shared with the Client. The CSP needs to update the system in response to any adverse findings in the report, without any additional cost to Client.
21. CSP shall be responsible for monitoring performance and service levels. CSP in coordination with MSI shall:
22. 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;
23. Review the service level reports, monitoring the service levels and identifying any deviations from the agreed service levels;
24. 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;
25. Detecting and reporting service level agreement infringements;
26. Monitoring of performance, resource utilization and other events such as failure of service, degraded service, availability of the network, storage, database systems, operating Systems, applications, including API access within the cloud service provider's boundary.

- CSP shall be responsible for the following usage reporting and billing management services:

27. Tracking system usage and usage reports;
28. Monitoring, managing and administering the monetary terms of SLAs and other billing related aspects;
29. Provide the relevant reports including real time as well as past data/information/reports for Client to validate the billing and SLA related penalties;
30. Optimize the overall cost to Client for cloud infrastructure usage for running its operations.

- MSI shall be responsible for configuring the infrastructure for back-up. Root Cause Analysis (RCA) of all incidents should be provided within 24 hours of the incident occurrence.
- CSP shall be responsible for following business continuity services:
- Provide business continuity services in case the system becomes unavailable.
- CSP shall support for third party audits and shall enable the logs and monitoring as required to support for third party audits.
- CSP shall ensure uptime and utilization of the cloud resources as per SLA's defined in this RFP.
- Upgrades: Any required version/Software /Hardware upgrades, patch management etc. at the Cloud Site shall be supported by the CSP for the entire contract period at no extra cost to the Client.
- CSP is required to provision additional VM's as per the auto-scaling rules defined in the Cloud Console in consultation with Client.
- CSP in coordination with MSI shall advise Client 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.
- Interface with the Cloud Service Provider(s) on behalf of Client for all activities including monitoring the reports (e.g. usage, security, SLA), raising (or escalating) tickets / incidents and tracking the same to resolution.
- Create and maintain all the necessary technical documentation, standard operating procedures, configurations required for continued operations and support of cloud services.
- MIS Reports - CSP shall submit the reports on a regular basis in a mutually decided format. The CSP shall workout the formats for the MIS reports and get these approved by the Client after award of the contract. The following is only an indicative list of MIS reports that may be submitted to the Client:

Monthly Reports

- Component wise server as well as Virtual machines availability and resource utilization;
- Consolidated SLA / Non- conformance report;
- Summary of component wise uptime;
- Log of preventive / scheduled maintenance undertaken;

- Log of break-fix maintenance undertaken;
- All relevant reports required for calculation of SLAs;
- Summary of issues / complaints logged with the OEMs;
- Summary of changes undertaken in the environment provisioned for Client including major changes like configuration changes, patch upgrades, etc. and minor changes like log truncation, volume expansion, user creation, user password reset, etc.;
- Summary of resolved, unresolved and escalated issues / complaints;
- Log of backup and restoration undertaken.
- Any other reports required by the Client

9.5 DRC / Secondary DC (DRC/Secondary DC shall only be applicable based upon approval from Client)

1. CSP shall be responsible for following business continuity services:
2. Provide business continuity services in case the primary site becomes unavailable.
3. Conduct secondary DC / DRC drill for two days (for the Client's environment), on the discretion of the Client, at the interval of every six months of operation wherein the Primary DC has to be deactivated and complete operations shall be carried out from the secondary DC / DRC Site. However, during the change from DC to secondary DC / DRC or vice-versa (regular planned changes), there should not be any data loss and should meet the RTO and RPO requirements. The CSP shall clearly define the procedure for announcing secondary DC / DRC based on the proposed secondary DC / DRC solution. The CSP shall also clearly specify the situations in which disaster shall be announced along with the implications of disaster and the time frame required for migrating to secondary DC / DRC. The CSP shall plan all the activities to be carried out during the Disaster Trial and issue a notice to the Client at least two weeks before such trial.

10 ROLES AND RESPONSIBILITIES

10.1 Cloud Service Provider (CSP)

Following are the responsibilities of the CSP:

A. CSP shall be responsible for provisioning the underlying system software, infrastructure, and cloud services for deployment and hosting of all the Client applications on the Infrastructure provided by MeitY empaneled Cloud Service Provider.
B. CSP in coordination with MSI shall be responsible for adequately sizing the necessary compute, memory, and storage required, building the redundancy into the architecture (including storage) and load balancing to meet the service levels mentioned in the RFP;
C. CSP shall coordinate with the MSI and e-LMS SI for migration and hosting of all applications to the proposed cloud platform.
D. The CSP shall be responsible for provisioning the necessary compute, memory, and storage as per the recommendations of the MSI and e-LMS SI.
E. For any additional software procured, the CSP shall provide the Annual Technical Support (ATS) from the CSP/OEM during the entire period of the contract.

10.2 Client - MITL

A. Assign a Project Manager with the authority to make decisions (and/or designate representatives with such authority) on behalf of Client.
B. Participate in all scheduled project activities, attend scheduled meetings and promptly respond to new meeting requests, requests for information, technical support or other necessary communication activities.
C. Timely acquisition of required technical data from MSI or other parties;
D. Obtaining any new, changed, or updated operational information necessary for the CSP to configure and initialize the system; and
E. Client shall have dedicated access to all virtual machines, templates, clones, and scripts/applications created for various applications, any user created/loaded data and applications hosted on CSP's infrastructure and maintains the right to request (or shall be able to retrieve) full copies of these virtual machines at any time.

10.3 Master System Integrator (MSI) and SI

A. MSI and e-LMS SI shall coordinate with CSP for hosting of e-gov and ERP applications, e-LMS and any other component.
B. MSI and e-LMS SI shall coordinate with CSP for migration of all MITL applications from existing cloud environment to the proposed Cloud Platform.
C. All application level redundancy, scalability, reliability etc. requirements shall be catered by MSI and e-LMS SI.
D. MSI shall be responsible for system architecture for cloud hosting. CSP shall assist MSI for the same.
E. MSI shall provide back-up and restoration services, specify/confirm RTO, RPO, clustering/high availability, single sign on, proposed application uptime, proposed application response time for all applications and their respective storage requirements.
F. MSI shall only be responsible for application level performance and uptime and not that of the availability of the infrastructure being provided by CSP. However, MSI shall be fully responsible to work hand in hand with the CSP and ensure that an overall highly available solution is provided for the Project.
G. All applications provided by MSI shall support auto-scaling.
H. All installation/operations, management and operations of the MSI provided applications

shall be performed by the MSI only. All managed services for installation shall be with MSI.

I. MSI shall be responsible for ensuring the optimised functioning of the infrastructure at any given time during the course of the Contract.
J. MSI shall provide managed services for operations and maintenance of the cloud infrastructure for all applications
K. MSI and e-LMS SI shall provide the application license and the database.

11 IMPLEMENTATION SCHEDULE

The tentative implementation schedule is provided in the table below.

Milestones indicated in the table below are indicative only and shall be read in conjunction with the CSP Scope of Services. Client and its authorized representative reserve the right to ask for additional information, deliverables and milestones during the course of the Contract.

Milestone	**Effective Date of Contract (D)**
Project Plan	D + 7 Days
Setting up cloud infrastructure for all the scope applications for the pre-production and production environments	D+15 Days
Successful Migration for e-LMS system, including operational acceptance testing, CDCPR-GIS, BPAS and GIS server	D + 30 Days
Successful Migration for other applications like electricity procurement, e-Gov and utility billing system	D+45 Days
Stabilisation and Operational Acceptance for Cloud Infrastructure	D+60 Days
Commencement of Operation and Maintenance Support Phase for Cloud Infrastructure**	D+60 Days
Completion of Operation and Maintenance Support Phase for Cloud Infrastructure	D+24 Months

**Note:

In case Migration and Operational Acceptance is delayed, the corresponding operations and maintenance support phase for Cloud Infrastructure will start after the Migration and Operational Acceptance have been completed

12 Special Terms and Conditions

General Conditions of Contract

A. GENERAL PROVISIONS

Relationship between the Parties	Nothing contained herein shall be construed as establishing a relationship of master and servant or of principal and agent as between the Client and the CSP. The CSP, subject to this Contract, has complete charge of the Personnel, if any, performing the Services required of CSP under this Contract and shall be fully responsible for the Services performed by them or on their behalf hereunder.
Governing Law	This Contract, its meaning and interpretation, and the relation between the Parties shall be governed by the Applicable Law.
Language	This Contract has been executed in the language specified in the SCC, which shall be the binding and controlling language for all matters relating to the meaning or interpretation of this Contract.
Headings	The headings are for convenience of reference only and shall not limit, alter or affect the meaning of this Contract.
Communications	Any communication, approval, notice, report, consent, certificate or request required or permitted to be given or made pursuant to this Contract ("**Communication**") shall be in writing in the language specified in the SCC. Unless otherwise specified in the Contract, any such Communication shall be sent by electronic mail or facsimile transmission, with a confirmation copy by courier or registered post to the address specified in the SCC. Any Communication sent by electronic mail or facsimile shall be deemed to have been received on the date of transmission and any notice served by courier or registered post shall be deemed to be received when actually delivered to the address specified in the SCC. A Party may change its address for Communication hereunder by giving the other Party notice of such change to the address specified in the SCC.
Authorized Representatives	Any action required or permitted to be taken, and any document required or permitted to be executed under this Contract by the Client or the CSP may be taken or executed by the officials specified in the SCC**.**
Corrupt and Fraudulent Practices	The CSP shall comply with the Client's policy in regard to corrupt and fraudulent practices as set forth in Attachment 1 to the GCC.
Commissions and Fees	The Client requires the CSP to disclose any commissions or fees that may have been paid or are to be paid to agents or any other party with respect to the selection process or execution of the Contract. The information disclosed must include at least the name and address of the agent or other party, the amount and currency, and the purpose of the commission, gratuity or fee. Failure to disclose such commissions, gratuities or fees may result in termination of the Contract.

B. COMMENCEMENT, COMPLETION, MODIFICATION AND TERMINATION OF CONTRACT

Effectiveness of Contract	This Contract shall come into force and effect on the date (the "Effective Date") Date of Contract Signing or 15 days from the date of issuance of Letter of Award (LOA) to the CSP, whichever is earlier
Commencement of Contract	The CSP shall submit in writing an acceptance of LOA and start the Project with Kick-off meeting no later than the date specified in the SCC.
Expiration of Contract	Unless terminated earlier pursuant to Clause 0, this Contract shall expire at the end of such time period after the Effective Date as specified in the SCC, unless extended in accordance with this Contract.
Entire Agreement	This Contract constitutes the entire understanding between the Parties regarding the scope of the System and supersedes all prior written or oral understandings, offers, agreements, communication or representations affecting the same subject matter. It is clarified that the obligations of the CSP under the RFP shall continue to subsist and shall be deemed to form part of the Contract.
Change or Modifications or Variations	Any change or modification or variation of the terms and conditions of this Contract, including any modification or variation of the scope of the System, may only be made by written agreement between the Parties. Both the Client and the CSP may, at any time during the term of the Contract, propose a variation to the System or Solution and/or any other provision of the Contract (Variation). No change made necessary because of any default of the CSP in the performance of its obligations under the Contract shall be deemed to be a Change, and such change shall not result in any adjustment of the Contract Price or the Time for Achieving Operational Acceptance or Expiration of Contract. *Client Proposed Variation:* The Client may, at any time during the term of the Contract, instruct the CSP, by issuing a written notice, to carry out a Variation (a **Variation Order**). Provided that, the Client shall not propose a Variation which is not technically or financially feasible, such feasibility being determined in accordance with Good Industry Practice, or any Variation that constitutes unrelated work; Within three (3) days of receipt of a Variation Order, the CSP shall submit a proposal setting out in sufficient detail the implications of the proposed Variation, including the (a) description of the work required or no longer required; (b) an estimate of the increase or decrease in the Total Value of Contract; (c) the Service Schedule; (d) Payment Schedule; Based on its review of the proposal submitted by the CSP, the Client may: (a) accept the proposal and the corresponding adjustments to the Total Value of Contract, Services Schedule, and Payment Schedule; (b) provide its comments on the proposal seeking amendments and/or justification for the implications put forth by the CSP; or (c) reject the proposal submitted by the CSP and withdraw the Variation Order, within seven (7) days from the date of receipt of the CSP's proposal under Clause 00; If the Client accepts the CSP's proposal under Clause 00 of this Section, it shall issue an instruction identifying the offer that is being accepted and requesting the CSP to proceed with the Variation. Upon the Client's acceptance of the CSP's proposal, the CSP shall proceed with the

	Variation; To the extent the Client seeks amendments and/or justification in the proposal submitted by the CSP, the CSP shall incorporate or address, in writing, the Client's comments and submit a revised proposal. On approval of the revised proposal in accordance with Clause 0 0, the CSP shall proceed with the Variation; On implementation of a Variation Order, the CSP shall be entitled to the agreed increase in the Total Value of Contract and/or adjustment to the Services Schedule or Payment Schedule for carrying out the Variation; Notwithstanding anything to the contrary in this Clause 0, the CSP shall be bound to implement any Variation that is necessitated by a Change in Law (*discussed in Clause 0 below*) and any consequent adjustment in the Total Value of Contract, Services Schedule or Payment Schedule, on account of such Variation, shall be determined in accordance with Clause *0* below; There shall be no restriction in terms of quantities in case of Client proposed variations. Client reserves the right to increase the cloud associated requirements up to any value; If in case Client procures additional cloud resources than the requirements provided in Financial Proposal Submission Forms – Recurring Costs – Form 1.5, Client shall procure as per the unit rates provided by the CSP in its financial proposal. Procurement will be governed as per pay-as-per-use model where Client may ask for additional cloud resources based on Client's requirements without any minimum bill or charges; If in case Client requires additional systems which are not a part of existing line items in the Financial Proposal (Financial Proposal Submission Forms – Recurring Costs – Form 1.5), then Client shall procure the systems as per the rate card provided as part of the (Financial Proposal Submission Forms —- Form 1.7. *CSP Proposed Variation:* The CSP may propose a Variation, which it considers necessary or desirable to improve the quality of the System and Solution to be deployed. While proposing a Variation, the CSP shall submit a proposal to the Client, with a statement setting out: (a) detailed particulars of the Variation; (b) the work required or no longer required; (c) an estimate of any adjustment in the Total Value of Contract; (d) any adjustment to the Services Schedule or Payment Schedule; and (e) any other effect the proposed Variation would have on any other provision of the Contract; Based on its review of the Variation proposed by the CSP, the Client may: (a) confirm the Variation; (b) provide its comments on the proposed Variation; or (c) reject the proposed Variation, while giving reasons in writing for such rejection, within seven (7) days of the submission of the proposal for a Variation. Upon the Client's acceptance of the proposed Variation, the CSP shall proceed with the Variation; To the extent the Client seeks amendments in the proposed Variation, the CSP shall incorporate or address, in writing, the Client's comments and submit a revised proposal. On approval of the revised proposal in accordance with Clause 00, the CSP shall proceed with the Variation; If the Parties are unable to reach agreement regarding the terms of a Variation Order, such disagreement shall be resolved pursuant to GCC

	Clause 0. Notwithstanding anything contained in this Clause 0, a Variation made necessary due to any act, omission or default of the CSP in the performance of its obligations under the Contract will not result in any increase in the Total Value of Contract or extension of any Deliverable/Milestone Due Date. No Variation invalidates the Contract. The CSP agrees that a Variation may involve the omission of any part of the Scope and further, the CSP agrees that the Client may engage others to perform that part of the Scope which has been omitted. The CSP further acknowledges that any omission or omissions will not constitute a basis to allege that the Client has repudiated the Contract no matter the extent or timing of the omission(s). Notwithstanding anything contained in this Clause 0, the Client shall not agree to any Variation if: (i) the CSP seeks any Variation in its obligations which is due to any shortcoming or deficiency in the documents provided by the CSP; (ii) the Variation relates to repeat performance of the Solution due to the CSP's failure to comply with the Client's requirements; or (iii) escalation in the cost of equipment, materials or the work force, other than on account of a Change in Law. *If due to any reason the CSP and Client are not able to finalize a change in the system (ex: including a hardware component, storage requirement or a software functionality which was not anticipated earlier), the Client reserves a right to get the change executed by any other third party. However the component or functionality being a part of the comprehensive system, the original CSP shall have obligation to support any integration effort required whatsoever and extend full co-operation to the third party and the Client.* The unit rates as indicated in the Contract shall be fixed during the CSP's performance of the Contract and shall not subject to increase on any account for any variation order during the currency of the Contract.
Change in Law	For the purposes of this Contract, "Change in Law" means the occurrence of any of the following events after the date of execution of the Contract: (i) the modification, amendment or repeal of any existing Applicable Law; (ii) the enactment, promulgation, bringing into effect, adoption of any new Applicable Law; (iii) change in the interpretation or application of any Applicable Law by any Authority; (iv) the introduction of a requirement for the CSP to obtain any new approval or permit or the unlawful revocation of an applicable approval or permit; or (v) the introduction of any new Tax or a change in the rate of an existing Tax. Change in Law does not include: (i) any change in the (Indian) Income Tax Act, 1961 with regard to the taxes on the income of the CSP; (ii) any statute that has been published in draft form or as a bill that has been placed before the legislature or that has been passed by the relevant legislature as a bill but has not come into effect prior to the date of the Contract and which is a matter of public knowledge; or (iii) a draft statutory instrument or delegated legislation that has been published prior to the date of the Contract, which is under the active consideration or contemplation of the GoI or GoM and which is a matter of public knowledge. If, after the date of this Contract, there is any Change in Law which:

	increases the cost incurred by the CSP in deploying the Project; and/or affects the Project Schedule. then the CSP may notify the Client and appropriate adjustments shall be made to the Total Value of Contract to account for the Change in Law. The notice shall be accompanied by all supporting documents, details and information required by the Client to assess the claims of the CSP. Provided that, if a Change in Law becomes applicable as a result of a delay by the CSP, then the CSP shall not be entitled to any adjustment in the Total Value of Contract and/or the Project Schedule. Where it is not possible to address the effect of a Change in Law (through an adjustment in the Total Value of Contract and/or the Project Schedule), the Parties shall agree on a mechanism, including amending the terms of the Contract, to mitigate the adverse effects of the Change in Law to CSP. If the Parties are unable to reach an agreement within thirty (30) days of the notification of a Change in Law, then the matter shall be referred to dispute resolution in accordance with GCC Clause 0.
Suspension	The Client may, by written notice of suspension to the CSP, suspend all payments to the CSP hereunder if the CSP fails to perform or is in breach of any of its obligations under this Contract, including the carrying out of the Services, provided that such notice of suspension: (i) shall specify the nature of the failure or breach, and (ii) shall request the CSP to remedy such failure within a period not exceeding thirty (30) calendar days after receipt by the CSP of such notice of suspension.
Termination	In case of any Contract Termination, the CSP shall be required to retain the Client data for a period of three (3) months and assist in any migration of data services as required by Client without any additional costs. This Contract may be terminated by either Party as per provisions set out below:
By the Client for CSP's default	A "CSP Event of Default" means any of the events set out below, unless such event has occurred as a consequence of a default by the Client as set out in GCC Clause 0, a Change in Law or any event of Force Majeure ("CSP Event of Default"): if the CSP fails to remedy a failure in the performance of its obligations hereunder, as specified in a notice of suspension pursuant to GCC Clause 0 within thirty (30) days of receipt of such notice of suspension or within such further period as the Client may have subsequently granted in writing; if the CSP becomes insolvent or bankrupt or enters into any agreements with its creditors for relief of debt or takes advantage of any law for the benefit of debtors or goes into liquidation or receivership whether compulsory or voluntary or, if the CSP is a corporation, a resolution is passed or order is made for its winding up; if the CSP's liability to pay delay liquidated damages reaches the cap on delay liquidated damages specified in GCC Clause 0 but the delay in respect of which the delay liquidated damages are payable continues to exist; If the CSP: has abandoned or repudiated the Contract;

	has without valid reason failed to commence work on the System promptly; persistently fails to execute the Contract in accordance with the Contract or persistently neglects to carry out its obligations under the Contract without just cause; refuses or is unable to provide sufficient Materials, Services, or labor to execute the system and offer services in the manner specified in the Agreed and Finalized Project Plan furnished under GCC Clause 0 at rates of progress that give reasonable assurance to the Client that the CSP can attain Operational Acceptance of the System by the Time for Achieving Operational Acceptance as extended; ***fails to provide sufficient Manpower, Material and Services during operations as required for meeting the SLA's specified in RFP (Service Level Agreement) during the Operations Period;*** ***If the penalties calculated as per SLA's specified in RFP Requirements (*Service Level Agreement), *exceed five percent (5%) of the quarterly payment Client owes to CSP for its Cloud and Managed services for that particular quarter except in case of security breach. Client reserves the right to terminate the Contract in case of any Security Breach.*** if the CSP has engaged in corrupt, fraudulent, collusive, coercive, undesirable or restrictive practice in competing for or in executing the Contract, including but not limited to willful misrepresentation of facts concerning ownership of Intellectual Property Rights in, or proper authorization and/or licenses from the owner to offer, the hardware, software, or materials provided under this Contract; if the CSP fails to furnish, renew and/or maintain the Performance Security in accordance with this Contract; if the CSP assigns or transfers the Contract or its rights and obligations under this Contract without the prior written consent of the Client; if any of the CSP's representations and warranties are found to be false and/or misleading; or if the CSP is in breach of any Applicable Laws; If the CSP or its CSP is blacklisted by any Govt. of India Authority to provide cloud services to Govt. bodies in India; If the CSP fails to achieve any cloud accreditation, empanelment or approval initiatives for its cloud services from the relevant Govt. of India Authority. Without prejudice to other provisions of this Contract, upon the occurrence of a CSP Event of Default, the Client may deliver a notice to the CSP specifying the nature of the breach and giving a cure period of thirty (30) days to the CSP to cure the CSP Event of Default. Provided that, in case of occurrence of a CSP Event of Default set out in Clauses 00, or 0 0, the Client shall have the right to terminate the Contract immediately, without any obligation to provide a cure period. Subject to Clause 0, and except in case of the event set out at Clause 0 0, if by the end of the cure period, the CSP has not remedied the CSP Event of Default or taken steps to remedy the CSP Event of Default to the satisfaction of the Client, then the Client shall have the right to issue

	a termination notice, upon which this Contract shall terminate forthwith. Upon receipt of the notice of termination under GCC Clause 0, the CSP shall, either immediately or upon such date as is specified in the notice of termination: cease all further services, except for such services as the Client may specify in the notice of termination for the sole purpose of protecting that part of the System already executed.; terminate all subcontracts, except those to be assigned to the Client pursuant to GCC Clause 00 below; to the extent legally possible, assign to the Client all right, title and benefit of the CSP to the System or Subsystems as at the date of termination, and, as may be required by the Client.; deliver to the Client all specifications, and other documents prepared by the CSP as at the date of termination in connection with the System. ***(a) If the termination takes place prior to the Expiration of the Contract, the CSP shall be entitled to be paid the Contract Price attributable to the portion of the System executed as on the date of termination and the costs, if any, incurred in protecting the System pursuant to GCC Clause 00. Any sums due to the Client from the CSP accruing prior to the date of termination shall be deducted from the amount to be paid to the CSP under the Contract.***
By the CSP for Client's default	A "Client Event of Default" means any of the following events set out below, unless such event has occurred as a consequence of a default by the CSP as set out in Clause 0, a Change in Law or any event of Force Majeure: if the Client fails to pay any undisputed money due to the CSP pursuant to this Contract within forty five (45) calendar days after receiving written notice from the CSP that such payment is overdue; if the Client is in material breach of its obligations under this Contract and has not remedied the same within forty five (45) days (or such longer period as the CSP may have subsequently approved in writing) following the receipt by the Client of the CSP's notice specifying such breach; if the CSP is unable to carry out any of its obligations under the Contract for any reason attributable to the Client, including but not limited to the Client's failure to provide any link with the applications or other areas or failure to obtain any governmental permit necessary for providing services as part of the System; if the Client becomes insolvent or bankrupt or enters into any agreements with its creditors for relief of debt or take advantage of any law for the benefit of debtors or goes into liquidation or receivership whether compulsory or voluntary; or, if the Client is a corporation, a resolution is passed or order is made for its winding up; if the Client suspends the performance of the Services for more than sixty (60) days, for reasons not attributable to the CSP. Without prejudice to other provisions of this Contract, upon the occurrence of a Client Event of Default, the CSP may deliver a notice to the Client specifying the nature of the breach and giving a cure period of thirty (30) days to the Client to cure the Client Event of Default. Provided that, in case of occurrence of a Client Event of Default set out

	in Clauses 00 or 0 0, the CSP shall have the right to terminate the Contract immediately, without any obligation to provide a cure period. If the Contract is terminated under GCC Clause 0, then the CSP shall immediately: cease all further services, except for such work as may be necessary for the purpose of protecting that part of the System;; terminate all subcontracts, except those to be assigned to the Client pursuant to Clause 00 0; In addition, the CSP, subject to the payment specified in GCC Clause 0, shall: to the extent legally possible, assign to the Client all right, title, and benefit of the CSP to the System, or Subsystems, as of the date of termination, and, as may be required by the Client; to the extent legally possible, deliver to the Client all specifications, and other documents prepared by the CSP as of the date of termination in connection with the System. If the Contract is terminated under GCC Clause 0, the Client shall pay to the CSP all payments specified in GCC Clause 0, and reasonable compensation for all loss, except for loss of profit, or damage sustained by the CSP arising out of, in connection with, or in consequence of such termination. Termination by the CSP pursuant to this GCC Clause 0 0 is without prejudice to any other rights or remedies of the CSP that may be exercised in lieu of or in addition to rights conferred by GCC Clause 0 0. In this GCC Clause 0, the expression “portion of the System executed” shall include all work executed, Services provided, (or subject to a legally binding obligation to purchase) by the CSP and used or intended to be used for the purpose of the System, up to and including the date of termination. In this GCC Clause 0, in calculating any monies due from the Client to the CSP, account shall be taken of any sum previously paid by the Client to the CSP under the Contract, including any advance payment paid pursuant to the SCC.
At Client’s convenience	The Client may at any time terminate the Contract for any reason by giving the CSP a notice of termination that refers to this GCC Clause 0 0. Upon receipt of the notice of termination under GCC Clause 0, the CSP shall either as soon as reasonably practical or upon the date specified in the notice of termination: cease all further services, except for such services as the Client may specify in the notice of termination for the sole purpose of protecting that part of the System already executed; terminate all subcontracts, except those to be assigned to the Client pursuant to GCC Clause 0 0 0 below; in addition, the CSP, subject to the payment specified in GCC Clause 0, shall to the extent legally possible, assign to the Client all right, title, and benefit of the CSP to the System, or Subsystem, as at the date of termination,

	and, as may be required by the Client; deliver to the Client all specifications, and other documents prepared by the CSP as of the date of termination in connection with the System; *If termination takes place after operational acceptance is achieved, the CSP shall fully comply with the Exit Management Plan as specified in Section E of GCC.* In the event of termination of the Contract under GCC Clause 0, the Client shall pay to the CSP the following amounts: **the *Contract Price, properly attributable to the parts of the System services executed by the CSP***; costs incurred by the CSP in protecting the System pursuant to GCC Clause 0 0; and the cost of satisfying all other obligations, commitments, and claims that the CSP may in good faith have undertaken with third parties in connection with the Contract and that are not covered by GCC Clause 0 0 through 0 above.
Termination for Force Majeure	If a Force Majeure event affecting any Party subsists for a continuous period of one hundred eighty (180) days, then either Party may issue a notice of termination to the other Party. Upon receipt of this notice, the Parties shall have a period of fifteen (15) days to agree on the manner in which the Contract may be progressed upon cessation of the Force Majeure event and the variations, if any, required to the Contract to address the consequences of the Force Majeure event. If on the expiry of the fifteen (15) day period, the Parties fail to arrive at an agreement, either Party may immediately terminate this Contract by written notice to the other Party.
Cessation of Rights and Obligations	Upon termination of this Contract pursuant to Clause 0, or upon expiration of this Contract pursuant to Clause 0, all rights and obligations of the Parties hereunder shall cease, except (i) any cause or action which may have occurred in favour of either Party or any right which is vested in either Party under any provision of the Contract as a result of any act, omission, deed, matter or thing done or omitted to be done by either Party before the expiry or termination of the Contract, (ii) the obligation of confidentiality set forth in Clause 0, (iii) the CSP's obligation to permit inspection, copying and auditing of their accounts and records set forth in Clause 0, (iv) the indemnity obligations of the Parties as set out in Clause 0; (v) the obligations in relation to intellectual property rights under Clause 0; and (vi) any right which a Party may have under the Applicable Law.
Cessation of Services	Upon termination of this Contract by either Party , the CSP shall: (i) immediately upon dispatch or receipt of such notice, take all necessary steps to bring the Services to a close in a prompt and orderly manner and shall make every reasonable effort to keep expenditures for this purpose to a minimum; and (ii) transfer to the Client all documents, data, programmes, applications, software, equipment etc. developed or acquired by the Client for the purposes of performing the System along with the right to use the Intellectual Property in such documents, data, programmes, applications, software, equipment for the Project.
Indemnity and	CSP's indemnity:

Limitation of Liability	The CSP must indemnify and hold harmless the Client and the Client's staff, their Affiliates and directors of their Affiliates (each a "Client Indemnified Party") from and against any and all claims and losses suffered or incurred by the Client Indemnified Party, including claims by a third party, arising out of: any failure of the CSP to pay taxes or any statutory dues; any non-compliance or violation of Applicable Law or applicable permits by the CSP; breach of the CSP's representations and warranties set out in the Contract; bodily injury, sickness or death of any person whatsoever engaged by CSP, Client or any of their subcontractor on the site during duty hours; breach of the CSP's obligations under the Contract; physical damage to the Project Office or any property therein; loss of or physical damage to property of any third party; or infringement of the Intellectual Property Rights of any third party by the CSP under the Contract. Client's indemnity: The Client agrees to indemnify and hold harmless the CSP and the Personnel (each a "CSP Indemnified Party") from and against any and all claims or losses suffered or incurred by the CSP Indemnified Party arising out of: breach of the Client's representations and warranties under the Contract; or any non-compliance or violation of Applicable Laws or any Client's applicable permits or consents by the Client. On receipt of a notice of any claim, which would entitle any Party ("Indemnified Party") to claim indemnification from the other Party ("Indemnifying Party"), the Indemnified Party shall, within a reasonable time, provide a written notice of the claim to the Indemnifying Party along with all the documents available with it in respect of the claim, specifying in detail the claim, the amount claimed by the third party, the date on which the claim arose and the nature of the default to which such claim relates (including a reference to the applicable provision of the Contract) and the Indemnifying Party shall settle the claim accordingly. The Indemnifying Party shall be entitled to but not obliged to participate in and control the defence of any such suit, action or proceeding at its own expense or direct the Indemnified Party to defend such claim, at the cost of the Indemnifying Party. If the Indemnifying Party elects to control the defence of any such suit, action or proceeding, the Indemnified Party shall render all necessary assistance for the purposes of enabling the Indemnifying Party to take the action referred to in this Clause 0. The Indemnifying Party may also request the Indemnified Party, at the cost of the Indemnifying Party to dispute, resist, appeal, compromise, defend, remedy or mitigate the matter or enforce against the third party the Indemnifying Party's rights in relation to the matter and in connection with proceedings related to the matter, use reputable advisers and lawyers chosen by the Indemnifying Party. The Indemnified Party shall not settle any such suit, action or proceeding without the prior written consent of

	the Indemnifying Party. The Indemnifying Party agrees and acknowledges that it shall fully indemnify the Indemnified Party for all amounts paid and/or costs incurred by the Indemnified Party in accordance with this Clause 0. Unless otherwise specified in the Contract, neither Party shall be liable to the other Party for any kind of indirect, punitive or consequential loss or damage or for any economic loss, loss of profit, loss of revenue, loss of use or business interruption which may be suffered by the other Party in connection with this Contract, except for losses caused by the fraud or wilful misconduct of the Party. The Party entitled to the benefit of an indemnity under this Clause 0 shall take all reasonable measures to mitigate any loss or damage which has occurred. If the Party fails to take such measures, the other Party's liabilities shall be correspondingly reduced. The obligation to indemnify stipulated in this Clause 0 is: continuing, separate and independent obligation of the Parties from their other obligations and shall survive the termination of this Contract; and shall not be limited or reduced by any insurance, except to the extent that the proceeds of any such insurance are capable of being applied to reduce claims made against the affected Party. For the purpose of this Clause 0: (i) “claim” means any claim, liability, proceeding, cause of action, action, suit, demand at law or in equity, in each case brought against either Party (including by any third party); and (ii) “loss” means all losses (excluding consequential losses, indirect losses and loss of profit), damages, liabilities, fines, interest, awards, penalties, costs (including, reasonable legal costs, lawyers' and arbitrators' fees), charges and expenses of whatever nature or howsoever occasioned including any of the above suffered by the non-defaulting Party or a third party as a result of any act or omission in the course of or in connection with the performance, non-performance or deficiency in the performance of obligations under this Contract.
Settlement of Disputes	Disputes shall be settled by arbitration in accordance with the following provisions: The seat of the arbitration shall be in India and the arbitration proceedings shall be held in Mumbai; The English language shall be the official language for all purposes; The arbitration shall be governed by the (Indian) Arbitration and Conciliation Act, 1996, as amended from time to time; Responsibility of payment for all costs of arbitration shall be as per the arbitration award; and The decision of the sole arbitrator or of a majority of the arbitrators (or of the third arbitrator if there is no such majority) shall be final and binding and shall be enforceable in any court of competent jurisdiction, and the Parties hereby waive any objections to or claims of immunity in respect of such enforcement.

C. RIGHTS AND OBLIGATIONS OF THE CSP

General	
Standard of Performance	The CSP shall perform the Services with all due diligence, efficiency and economy, in accordance with Best Industry Practices and this Contract, and shall observe sound management practices, and employ appropriate information technologies, systems, support, maintenance, training and other related services or in accordance with Best Industry Practices. In particular, the CSP shall provide and employ only technical personnel who are skilled and experienced in their respective callings and supervisory staff who are competent to adequately supervise the work at hand. The CSP confirms that it has entered into this Contract on the basis of a proper examination of the data relating to the System provided by the Client and of other data readily available to the CSP relating to the System as at the date twenty-eight (28) days prior to bid submission. The CSP acknowledges that any failure to acquaint itself with all such data and information shall not relieve its responsibility for properly estimating the difficulty or cost of successfully performing the Contract. The CSP shall be responsible for timely provision of all resources, information, and decision making under its control that are necessary to reach a mutually Agreed and Finalized Project Plan (pursuant to GCC Clause 0) within the time schedule specified in the Implementation Schedule in the Terms of Reference Section. Failure to provide such resources, information, and decision making may constitute grounds for termination pursuant to GCC Clause 0 0. The CSP shall adhere to the SLA requirements as specified in RFP. The CSP shall not subcontract (unless otherwise specified in the SCC) any part of the Services required of CSP under this Contract. Other obligations of the Bidder as specified in SCC.
Law Applicable	The CSP shall comply with all laws in force in India. The laws will include all national, provincial, municipal, or other laws that affect the performance of the Contract and are binding upon the CSP. The CSP shall indemnify and hold harmless the Client from and against any and all liabilities, damages, claims, fines, penalties, and expenses of whatever nature arising or resulting from the violation of such laws by the CSP or its personnel, but without prejudice to GCC Clause 0. The CSP shall not indemnify the Client to the extent that such liability, damage, claims, fines, penalties, and expenses were caused or contributed to by a fault of the Client. Throughout the duration of the Contract, the CSP shall comply with the prohibitions in India in relation to the import of goods and services when as a matter of law or official regulation, there is a prohibition on entering into or maintaining commercial relations with the country from where the import is proposed to be made. The CSP shall acquire in its name all permits, approvals, and/or licenses from all local, state, or national government authorities or public service undertakings that are necessary for the performance of the Contract, including, without limitation, visas for the CSP's personnel and entry permits for all imported CSP's Equipment. The CSP shall acquire all other permits, approvals, and/or licenses that are not the responsibility of the Client under GCC Clause 0 and that are necessary for the performance

	of the Contract.
Conflict of Interest	The CSP shall hold the Client's interests paramount, without any consideration for future work, and strictly avoid conflict with other assignments or their own corporate interests.
CSP Not to Benefit from Commissions, Discounts, etc.	The Contract Price pursuant to GCC Clause 0 shall constitute the CSP's only payment in connection with this Contract and the CSP shall not accept for its own benefit any trade commission, discount or similar payment in connection with activities pursuant to this Contract or in the discharge of its obligations hereunder, and the CSP shall use its best efforts to ensure that the Personnel and agents or either of them, similarly shall not receive any such additional payment.
CSP and Affiliates Not to Engage in Certain Activities	The CSP agrees that, during the term of this Contract and after its termination/completion, the CSP and its Affiliates, shall be disqualified from providing consultancy related to the Services, for the implementation of the cloud and managed services, unless otherwise indicated in the SCC.
Prohibition of Conflicting Activities	The CSP shall not engage, and shall cause its Personnel to not engage, either directly or indirectly, in any business or professional activities that would conflict with the activities assigned to them under this Contract.
Strict Duty to Disclose Conflicting Activities	The CSP has an obligation and shall ensure that its Personnel shall have an obligation to disclose any situation of actual or potential conflict that impacts their capacity to serve the best interest of the Client, or that may reasonably be perceived as having this effect. Failure to disclose said situations may lead to the disqualification of the CSP or the termination of this Contract.
Confidentiality	Except with the prior written consent of the Client, the CSP and the Personnel shall not at any time communicate to any person or entity any proprietary or confidential information, including information relating to reports, data, design software or other material, whether written or oral, in electronic or magnetic format, and the contents thereof; and any reports, digests or summaries created or derived from any of the foregoing that is provided by the Client to the Personnel; any information provided by or relating to the Client, its technology, technical processes, business affairs or finances or any other information acquired in the course of the Services, nor shall the CSP and the Personnel make public the recommendations formulated in the course of, or as a result of, the Solution subject to: all Confidential Information shall be identified as confidential at the time of disclosure; each Party will comply with all applicable export and import laws and associated embargo and economic sanction regulations, applicable to either Party, that prohibit or restrict the export, re-export, or transfer of products, technology, services or data, directly or indirectly, to certain countries, or for certain end uses or end users. Notwithstanding the aforesaid, the CSP and the Personnel may disclose such information to the extent that such information: was in the public domain prior to its delivery to the CSP/Personnel or becomes a part of the public domain from a source other than the

	CSP/Personnel; was obtained from a third party with no known duty to maintain its confidentiality; is required to be disclosed under Applicable Laws or judicial/ administrative/arbitral process or by any government instrumentality, provided that such disclosure is made: (a) after giving a prior written notice to the Client; and (b) using reasonable efforts to ensure that such disclosure is accorded confidential treatment; is provided to the professional advisers, agents, auditors or representatives of the CSP on a needs basis as is reasonable under the circumstances, provided that the CSP shall require such professional advisers, agents, auditors or representatives to undertake in writing to keep the information provided confidential, and further provided that the CSP shall use best efforts to ensure compliance with such undertaking; is independently developed by the recipient or is already in the possession of the recipient.
Liability of the CSP	Subject to the exclusions set out in the SCC, the overall liability of the CSP and the Client under this Contract shall not exceed the total cost of Performance Security required as part of the RFP, provided that this limitation shall not apply to any obligation of the CSP to indemnify the Client with respect to intellectual property rights infringement.
Insurance to be Taken out by the CSP	The CSP shall at its expense take out and maintain in effect, or cause to be taken out and maintained in effect, during the performance of the Contract, the insurance set forth below. The identity of the insurers and the form of the policies shall be subject to the approval of the Client, who should not unreasonably withhold such approval. Third-Party Liability Insurance On terms as **specified in the SCC,** covering bodily injury or death suffered by third parties (including the Client's personnel) and loss of or damage to property (including the Client's property and any Subsystems that have been accepted by the Client) occurring in connection with the supply and installation of the Information System. Other Insurance (if any), as **specified in the SCC.** The CSP shall deliver to the Client certificates of insurance (or copies of the insurance policies) as evidence that the required policies are in full force and effect. If the CSP fails to take out and/or maintain in effect the insurance referred to in GCC Clause 0, the Client may take out and maintain in effect any such insurance and may from time to time deduct from any amount due the CSP under the Contract any premium that the Client shall have paid to the insurer or may otherwise recover such amount as a debt due from the CSP. Unless otherwise provided in the Contract, the CSP shall prepare and conduct all and any claims made under the policies effected by it pursuant to this GCC Clause 0, and all monies payable by any insurers shall be paid to the CSP. The Client shall give to the CSP all such reasonable assistance as may be required by the CSP in connection with any claim under the relevant insurance policies. With respect to insurance claims in which the Client's interest is involved, the CSP shall not give any release

	or make any compromise with the insurer without the prior written consent of the Client. With respect to insurance claims in which the CSP's interest is involved, the Client shall not give any release or make any compromise with the insurer without the prior written consent of the CSP.
Accounting, and Auditing	The CSP shall keep accurate and systematic accounts and records in respect of the Services required of CSP under this Contract, in accordance with internationally accepted accounting principles and in such form and detail as will clearly identify all relevant time charges and costs and the basis thereof. The CSP shall permit, the Client and/or persons appointed by the Client to inspect all accounts and records relating to the performance of the Contract, and to have such accounts and records audited by auditors appointed by the Client, if requested by the Client. Any act intended to materially impede the exercise of the Client's inspection and audit rights provided for under this Clause 0 shall constitute a material breach of the Contract, which would give the Client the right to terminate the Contract.
Time for Commencement and Operational Acceptance	The CSP shall commence work on the System within the period specified in the SCC, and without prejudice to GCC Clause 0, the CSP shall thereafter proceed with the System in accordance with the time schedule specified in the Implementation Schedule in the Terms of Reference Section and the Agreed and Finalized Project Plan. The CSP shall achieve Operational Acceptance of the System (or Subsystem(s) where a separate time for Operational Acceptance of such Subsystem(s), if provided, is specified in the Contract) within the time specified in the SCC and in accordance with the time schedule specified in the Implementation Schedule in the Terms of Reference Section and in the Agreed and Finalized Project Plan, or within such extended time to which the CSP shall be entitled under GCC Clause 0 (Extension of Time for Achieving Operational Acceptance).

D. PERSONNEL

Description of Key Experts	The title, agreed job description and minimum qualification of each Key Expert to carry out the Work are described in Professional Qualification Document All Key Experts as proposed by the Bidder should be full time employees of the Bidder.
Replacement of Key Experts	Except as the Client may otherwise agree in writing and no changes shall be made in the Key Experts without the prior consent of the Client. A request for substitution of a Key Expert during the term of the Contract may be considered based on the CSP's written request. The Client may make a request in writing for the substitution of a Key Expert with an equal or better qualification and experience. On receiving request, the CSP shall provide substitution within 30 days of receipt of request for the respective Key Expert. In case any proposed resource resigns, then the CSP has to inform Client within one week of such resignation and the CSP shall promptly initiate a search for a replacement to ensure that the role of any member of the Key Personnel is not vacant at any point in time during the contract period, subject to reasonable extensions requested by the CSP and its

	approval by the Client. If Client objects to any such replacement appointment, the CSP shall not assign the individual to that position and shall seek an alternative candidate in accordance with the resource requirements. The CSP needs to ensure at least 4 weeks of overlap period in such replacements. Client will not be responsible for any knowledge transition to the replacement resource and any impact/escalation of cost incurred by the CSP due to resource replacement.
Removal of Personnel	If the Client finds that any of the Personnel has committed serious misconduct or has been charged with having committed a criminal action, or if the Client determines that CSP's Personnel have engaged in any corrupt, fraudulent, coercive, collusive, undesirable or restrictive practices (as specified in Attachment 1 to the GCC) while performing the Work, the CSP shall, at the Client's written request, provide a replacement for such Personnel. In the event that any of Personnel is found by the Client to be incompetent or incapable in discharging assigned duties, the Client, specifying the grounds therefore, may request the CSP to provide a replacement. The replacement of any Personnel shall possess equivalent or better qualifications and experience and shall be approved by the Client.

E. EXIT MANAGEMENT AFTER OPERATIONAL ACCEPTANCE

Under Contract Completion	Provide a comprehensive exit management plan to MITL with a recommended "Exit Management SOP" within 90 days of signing of the contract. The CSP shall fully train Client's staff or any other agency designated by Client who is designated to take over the operations of the System. The CSP shall be responsible for transferring all the knowledge regarding the Systems, technically and operationally to enable the new agency/ Client to carry out the requisite functions. All latest operations & technical manuals, documentation, configuration files, software, licenses, etc. shall be handed over to Client at least 1 months before contract expiration. The CSP shall be responsible for providing the tools for import / export of VMs & content and the CSP shall be responsible for preparation of the Exit Management Plan and carrying out the exit management / transition. Also, CSP shall retain all Client data for a period of three (3) months without any additional cost to the Client. CSP shall be responsible for 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 Client'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 industry standard media; The format of the data transmitted from the cloud service provider to the new environment created by the Client should leverage standard data formats (e.g., OVF) whenever possible to ease and enhance portability. The format will be finalized by the Client;

	The CSP will transfer the organizational structure developed during the Contract Duration to support the delivery of the Exit Management Services. This will include: Document, update, and provide functional organization charts, operating level agreements with Third-Party contractors, phone trees, contact lists, and standard operating procedures. Transfer physical and logical security processes and tools, including cataloguing and tendering all badges and keys, documenting ownership and access levels for all passwords, and instructing Client or its authorized representative in the use and operation of security controls. Retain the data at the end of the Contract; 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 Client; It may be possible at any time to move the Cloud Virtual Machines to the Client or any other Infrastructure as service provider. The mechanism and technical requirements for achieving this shall be well documented; Client shall release the performance security to the CSP only after satisfactory Exit Management is achieved as part of the project and CSP is obligated to perform all required additional functions to facilitate the same for a smooth transfer of the duties. The Parties may, if mutually agreed, extend the contract in accordance with the terms and conditions **as specified in the SCC.** The ownership of the data generated upon usage of the system, at any point of time during the Contract or expiration of the Contract, shall rest absolutely with Client.
Under Termination upon CSP's Default / Client's Convenience (as per GCC Clauses 15 (a) and 15 (c))	Provide a comprehensive exit management plan; After termination notice by the Client, the CSP shall as soon as possible fully train Client's staff or any other agency designated by Client who is designated to take over the operations of the System. The CSP shall be responsible for continuing the services as per the scope of the contract during the Termination period as per the SLA's in the RFP. The CSP shall be responsible for transferring all the knowledge regarding the Systems, technically and operationally to enable the new agency/ Client to carry out the requisite functions. All latest operations & technical manuals, documentation, configuration files, software, licenses, etc. shall be handed over to Client at least 1 months before contract expiration. The CSP shall be responsible for providing the tools for import / export of VMs & content and the CSP shall be responsible for preparation of the Exit Management Plan and carrying out the exit management / transition. Also, CSP shall retain all Client data for a period of three (3) months without any additional cost to the Client. CSP shall be responsible for 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 Client'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 industry standard media; The format of the data transmitted from the cloud service provider to the new environment created by the Client should leverage standard data formats (e.g., OVF) whenever possible to ease and enhance portability. The format will be finalized by the Client; The CSP will transfer the organizational structure developed during the Contract Duration to support the delivery of the Exit Management Services. This will include: Document, update, and provide functional organization charts, operating level agreements with Third-Party contractors, phone trees, contact lists, and standard operating procedures. Transfer physical and logical security processes and tools, including cataloguing and tendering all badges and keys, documenting ownership and access levels for all passwords, and instructing Client or its authorized representative in the use and operation of security controls. Retain the data at the end of the Contract; 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 Client; It may be possible at any time to move the Cloud Virtual Machines to the Client or any other Infrastructure as service provider. The mechanism and technical requirements for achieving this shall be well documented; Client shall release the requisite payments to the CSP pursuant to the GCC/SCC Clause 0 to the CSP only after satisfactory Exit Management is achieved as part of the project and CSP is obligated to perform all required additional functions to facilitate the same for a smooth transfer of the duties. The ownership of the data generated upon usage of the system, at any point of time during the Contract or Termination of the Contract, shall rest absolutely with the Client.

F. RIGHTS AND OBLIGATIONS OF THE CLIENT

Assistance and Services	Unless otherwise specified in the SCC, the Client shall: Assist the CSP with obtaining any applicable permits, including work permits and such other documents as shall be necessary to enable the CSP to perform the Services required of CSP under this Contract; The Client shall be responsible for timely provision of all resources, information, and decision making under its control that are necessary to reach an Agreed and Finalized Project Plan (pursuant to GCC Clause 0) within the time schedule specified in the Implementation Schedule in the Terms of Reference Section. If requested by the CSP, the Client shall use its best endeavors to assist the CSP in obtaining in a timely and expeditious manner all permits, approvals, and/or licenses necessary for the execution of the Contract from all local, state, or national government authorities or public service undertakings that such authorities or undertakings require the CSP or the personnel of the CSP, as the case may be, to obtain. In such cases where the responsibilities of specifying and acquiring or

	upgrading telecommunications and/or electric power services falls to the CSP, as specified in the Terms of Reference, SCC, Agreed and Finalized Project Plan, or other parts of the Contract, the Client shall use its best endeavors to assist the CSP in obtaining such services in a timely and expeditious manner. The Client shall be responsible for timely provision of all resources, access, and information necessary for the Installation and Operational Acceptance of the System (including, but not limited to, any required telecommunications or electric power services), as identified in the Agreed and Finalized Project Plan, except where provision of such items is explicitly identified in the Contract as being the responsibility of the CSP. Delay by the Client may result in an appropriate extension of the Time for Operational Acceptance, at the CSP's discretion. The Client assumes primary responsibility for the Operational Acceptance Test(s) for the System, in accordance with GCC Clause 0. However, this shall not limit in any way the CSP's responsibilities after the date of Operational Acceptance otherwise specified in the Contract. The CSP is responsible for performing and safely storing timely and regular backups of its data and Software in accordance with accepted data management principles. All costs and expenses involved in the performance of the obligations under this GCC Clause 0 shall be the responsibility of the Client, save those to be incurred by the CSP with respect to the performance of the Operational Acceptance Test(s), in accordance with GCC Clause 0. The Client may depute Project Management Consultant (PMC) or competent personnel to properly carry out Pre-commissioning, Installation, Commissioning, and Operational Acceptance, at or before the time specified in the Terms of Reference Section's Implementation Schedule and the Agreed and Finalized Project Plan. Provide to the CSP any such other assistance as may be specified in the SCC.
Counterpart Personnel	Unless otherwise specified in the Contract or agreed upon by the Client and the CSP, the Client shall provide sufficient, properly qualified operating and technical personnel, as required by the CSP to properly carry out Pre-commissioning, Installation, Commissioning, and Operational Acceptance, at or before the time specified in the Terms of Reference Section's Implementation Schedule and the Agreed and Finalized Project Plan. The Client will designate appropriate staff for the training courses to be given by the CSP and shall make all appropriate logistical arrangements for such training as specified in the Terms of Reference, SCC, the Agreed and Finalized Project Plan, or other parts of the Contract.

G. PAYMENTS TO THE CSP

Total Value of the Contract	Clause Deleted. The Contract Price shall be aggregate of One Time Costs (which will be paid on completion of milestones) and Recurring Costs, paid quarterly, as specified in the Financial Proposal. The recurring cost shall be based on pay as per use model where unit prices committed by CSP as specified in the Recurring Costs of the Financial Proposal shall prevail during the Contract. The system requirements presented as part of Financial Proposal is for price discovery and evaluation purpose only and will not infer any commercial commitment to the CSP. Price discovery is done only for payment to CSP on the basis Pay as per use model based on consumption of cloud resources by the Client. Other conditions and obligations of the CSP associated with Total Value of Contract and Terms of Payment including negotiations shall be in accordance with GCC clause 0. The Contract price shall be as per pay as per use model and not be subject to any alternation, except: in the event of a Change in the System pursuant to GCC Clause 0 or to other clauses in the Contract; in accordance with the price adjustment formula (if any) **specified in the SCC.** The CSP shall be deemed to have satisfied itself as to the correctness and sufficiency of the Contract Price, which shall, except as otherwise provided for in the Contract, cover all its obligations under the Contract.
Taxes and Duties	The CSP is responsible for meeting any and all Tax liabilities arising out of the Contract in India or elsewhere, unless it is stated otherwise in the SCC. All payments made by the Client to the CSP shall be subject to deductions and withholding of applicable Taxes in accordance with Applicable Laws. If any tax exemptions, reductions, allowances, or privileges may be available to the CSP in the Client's Country, the Client shall use its best efforts to enable the CSP to benefit from any such tax savings to the maximum allowable extent. For the purpose of the Contract, it is agreed that the Contract Price as specified in Contract Agreement is inclusive of all taxes, duties, levies, and charges prevailing at the date twenty-eight (28) days prior to the date of bid submission in the Client's Country. If any Tax rates are increased or decreased, a new Tax is introduced, an existing Tax is abolished, or any change in interpretation or application of any Tax occurs in the course of the performance of the Contract, which was or will be assessed on the CSP, or their employees in connection with performance of the Contract, an equitable adjustment to the Contract Price shall be made to fully take into account any such change by addition to or reduction from the Contract Price, as the case may be.
Currency of Payment	Any payment under this Contract shall be made in Indian Rupees (INR).
Securities	Issuance of Securities The CSP shall provide the securities specified below in favor of the Client at the times and in the amount, manner, and form specified below.

	Performance Security: The CSP shall, within thirty (30) days of the notification of Contract award, provide a security for the due performance of the Contract in the amount and currency **specified in the SCC;** The security shall be a bank guarantee in the form provided in the Sample Forms Section of the Bidding Documents, or it shall be in another form acceptable to the Client; The security shall automatically become null and void once all the obligations of the CSP under the Contract have been fulfilled. The security shall be returned to the CSP no later than twenty-eight (28) days after its expiration;
Mode of Billing and Payment	The CSP's request for payment shall be made to the Client in writing, accompanied by an invoice describing, as appropriate, the System, along with proof of usage of services upon fulfilment of other obligations stipulated in the Contract and as per pay as you use model. The Contract Price shall be paid as **specified in the SCC.** Payments shall be made promptly by the Client, but in no case later than forty five (45) days after submission of a valid invoice by the CSP. Notwithstanding anything to the contrary in the Contract, the Client may withhold from any payment due to the CSP any amounts that the Client deems reasonably necessary or appropriate because of any one or more of the following reasons: Any penalties applicable on the CSP as per SLA; Failure by the CSP to provide certificates of insurance; Any overpayments made by the Client in a previous payment; Any payment required to be withheld under any Applicable Law; The invoice is not accompanied by all necessary supporting documents; A dispute exists as to the accuracy or completeness of any invoice; or Any amounts due to the Client from the CSP under the Contract. All payments under this Contract shall be made by wire transfer to the accounts of the CSP specified in the SCC.

H. INTELLECTUAL PROPERTY

Copyright	The Intellectual Property Rights in all Standard Software and Standard Materials shall remain vested in the owner of such rights. The Client agrees to restrict use, copying, or duplication of the Standard Software and Standard Materials in accordance with GCC Clause 0, except that additional copies of Standard Materials may be made by the Client for use within the scope of the project of which the System is a part, in the event that the CSP does not deliver copies within thirty (30) days from receipt of a request for such Standard Materials. *The Client may assign, license, or otherwise voluntarily transfer its contractual rights to use the Standard Software or elements of the Standard Software, without the CSP's prior written consent, under the following circumstances:*

	To any agency that shall be responsible to operate the project in the future in the event of dilution of the Client or the responsibility being transferred from Client to other agency; *In the event of termination of contract.* *The CSP shall protect the Client from any liabilities arising there from. The CSP shall indicate all those components in the software, if any, that cannot be bound by this condition explicitly while responding to the bid, and supporting with the corresponding evidence for the same.* As applicable, the Client's and CSP's rights and obligations with respect to Custom Software or elements of the Custom Software, including any license agreements, and with respect to Custom Materials or elements of the Custom Materials, are specified in the SCC**. Subject to the SCC,** the Intellectual Property Rights in all Custom Software and Custom Materials specified in the Contract Agreement (if any) shall, at the date of this Contract or on creation of the rights (if later than the date of this Contract), vest in the Client. The CSP shall do and execute or arrange for the doing and executing of each necessary act, document, and thing that the Client may consider necessary or desirable to perfect the right, title, and interest of the Client in and to those rights. In respect of such Custom Software and Custom Materials, the CSP shall ensure that the holder of a moral right in such an item does not assert it, and the CSP shall, if requested to do so by the Client and where permitted by applicable law, ensure that the holder of such a moral right waives it. The Parties shall enter into such (if any) escrow arrangements in relation to the Source Code to some or all of the Software as are **specified in the SCC** and in **accordance with the SCC.**
Software License Agreements	Except to the extent that the Intellectual Property Rights in the Software vest in the Client, the CSP hereby grants to the Client license to access and use the Software, including all inventions, designs, and marks embodied in the Software. All software licenses and applications specific to this Project (as applicable) shall be provided with perpetual, royalty free licenses. Such license to access and use the Software shall: be: nonexclusive; *fully paid up and irrevocable (except that it shall terminate if the Contract terminates before its expiration pursuant to GCC Clauses 0 0 and 0 0*; valid throughout the territory of the Client's Country; and permit the Software to be: used or copied for use on or with the computer(s) for which it was acquired (if specified in the Terms of Reference and/or the CSP's bid), plus a backup computer(s) of the same or similar capacity, if the primary is(are) inoperative, and during a reasonable transitional period when use is being transferred between primary and backup; *the Software license shall permit the Software to be used or copied for use or transferred to a replacement computer:* ***provided the replacement computer falls within approximately the same or a higher class of machine and maintains approximately the same***

	number of users, if a multi-user machine; if the nature of the System is such as to permit such access, accessed from other computers connected to the primary and/or backup computer(s) by means of a local or wide-area network or similar arrangement, and used on or copied for use on those other computers to the extent necessary to that access; reproduced for safekeeping or backup purposes; customized, adapted, or combined with other computer software for use by the Client, provided that derivative software incorporating any substantial part of the delivered, restricted Software shall be subject to same restrictions as are set forth in this Contract; *the Software license shall permit the Software to be disclosed to and reproduced for use (including a valid sublicense) by**: support service CSPs, exclusively for such CSPs in the performance of their support service contracts,** subject to the same restrictions set forth in this Contract;* *In addition to the persons specified in GCC Clause 0 0 0, the Software may be disclosed to, and **reproduced** for use by, **Client or its SPV entities or any other party which would take over the project in the future** subject to the same restrictions as are set forth in this Contract.* The CSP's right to audit the Standard Software will be subject to the following terms: *Maximum of 1 audit per calendar year is allowed by the Client and the duration of such audit shall not exceed 3 consecutive working days;* *The CSP shall get a prior written approval from Maharashtra Industrial Township Limited (MITL) at least 1 week in advance on the nature, number of people and duration of the audit.* *The Client does not have any financial implication for conducting any such audit and can only extend necessary logistic support pertaining to relevant technical man power resources.*
Confidential Information	The "Receiving Party" (either the Client or the CSP) shall keep confidential and shall not, without the written consent of the other party to this Contract ("the Disclosing Party"), divulge to any third party any documents, data, or other information of a confidential nature ("Confidential Information") connected with this Contract, and furnished directly or indirectly by the Disclosing Party prior to or during performance, or following termination, of this Contract. For the purposes of GCC Clause 0, the CSP is also deemed to be the Receiving Party of Confidential Information generated by the CSP itself in the course of the performance of its obligations under the Contract and relating to the businesses, finances, CSPs, employees, or other contacts of the Client or the Client's use of the System. Notwithstanding GCC Clauses 0 and 0: The Client may furnish Confidential Information of the CSP: (i) to its support service CSPs to the extent reasonably required for them to perform their work under their support service contracts; and (ii) to its affiliates and subsidiaries, in which event the Receiving Party shall ensure that the person to whom it furnishes Confidential Information of the Disclosing Party is aware of

	and abides by the Receiving Party's obligations under this GCC Clause 0 as if that person were party to the Contract in place of the Receiving Party. The Client shall not, without the CSP's prior written consent, use any Confidential Information received from the CSP for any purpose other than the operation of the System. Similarly, the CSP shall not, without the Client's prior written consent, use any Confidential Information received from the Client for any purpose other than those that are required for the performance of the Contract. The obligation of a party under GCC Clause 0 through 0 above, however, shall not apply to that information which: now or hereafter enters the public domain through no fault of the Receiving Party; can be proven to have been possessed by the Receiving Party at the time of disclosure and that was not previously obtained, directly or indirectly, from the Disclosing Party; otherwise lawfully becomes available to the Receiving Party from a third party that has no obligation of confidentiality. The above provisions of this GCC Clause 0 shall not in any way modify any undertaking of confidentiality given by either of the Parties to this Contract prior to the date of the Contract in respect of the System or any part thereof. The provisions of this GCC Clause 0 shall survive the termination, for whatever reason, of the Contract for three (3) years or such longer period as may be **specified in the SCC.**

I. INSTALLATION, TESTING, COMMISSIONING, AND ACCEPTANCE OF THE SYSTEM

Representatives	Project Manager If the Project Manager is not named in the Contract, then within fourteen (14) days from the Effective Date, the Client shall appoint and notify the CSP in writing of the name of the Project Manager. The Client may from time to time appoint some other person as the Project Manager in place of the person previously so appointed and shall give a notice of the name of such other person to the CSP without delay. No such appointment shall be made at such a time or in such a manner as to impede the progress of work on the System. Such appointment shall take effect only upon receipt of such notice by the CSP. Subject to the extensions and/or limitations **specified in the SCC** (if any), the Project Manager shall have the authority to represent the Client on all day-to-day matters relating to the System or arising from the Contract, and shall normally be the person giving or receiving notices on behalf of the Client. CSP's Representative If the CSP's Representative is not named in the Contract, then within fourteen (14) days of the Effective Date, the CSP shall appoint the CSP's Representative and shall request the Client in writing to approve the person so appointed. The request must be accompanied by a detailed curriculum vitae for the nominee, as well as a description of any other System or non-System responsibilities the nominee would retain while performing the duties of the CSP's Representative. If the Client does not object to the appointment within fourteen (14) days, the CSP's

	Representative shall be deemed to have been approved. If the Client objects to the appointment within fourteen (14) days giving the reason therefore, then the CSP shall appoint a replacement within fourteen (14) days of such objection in accordance with this GCC Clause 0; Subject to the extensions and/or limitations **specified in the SCC** (if any), the CSP's Representative shall have the authority to represent the CSP on all day-to-day matters relating to the System or arising from the Contract, and shall normally be the person giving or receiving notices on behalf of the CSP; The CSP shall not revoke the appointment of the CSP's Representative without the Client's prior written consent, which shall not be unreasonably withheld. If the Client consents to such an action, the CSP shall appoint another person of equal or superior qualifications as the CSP's Representative, pursuant to the procedure set out in GCC Clause 0; The CSP's Representative and staff are obliged to work closely with the Client's Project Manager and staff, act within their own authority, and abide by directives issued by the Client that are consistent with the terms of the Contract. The CSP's Representative is responsible for managing the activities of its personnel and any subcontracted personnel; The CSP's Representative may, subject to the approval of the Client (which shall not be unreasonably withheld), at any time delegate to any person any of the powers, functions, and authorities vested in him or her. Any such delegation may be revoked at any time. Any such delegation or revocation shall be subject to a prior notice signed by the CSP's Representative and shall specify the powers, functions, and authorities thereby delegated or revoked. No such delegation or revocation shall take effect unless and until the notice of it has been delivered; Any act or exercise by any person of powers, functions and authorities so delegated to him or her in accordance with GCC Clause 0 shall be deemed to be an act or exercise by the CSP's Representative. Objections and Removals The Client may by notice to the CSP object to any representative or person employed by the CSP in the execution of the Contract who, in the reasonable opinion of the Client, may have behaved inappropriately, be incompetent, or be negligent. The Client shall provide evidence of the same, whereupon the CSP shall remove such person from work on the System; If any representative or person employed by the CSP is removed in accordance with GCC Clause 0, the CSP shall, where required, promptly appoint a replacement.
Project Plan	In close cooperation with the Client and based on the Preliminary Project Plan included in the CSP's bid, the CSP shall develop a Project Plan encompassing the activities specified in the Contract. The contents of the Project Plan shall be as **specified in the SCC** and/or Technical Requirements. The CSP shall formally present to the Client the Project Plan in accordance with the procedure specified in the SCC. If required, the impact on the Implementation Schedule of modifications agreed during finalization of the Agreed and Finalized Project Plan shall be incorporated in the Contract by amendment, in accordance with GCC

	Clauses 0 and 0. The CSP shall undertake to all the services envisaged as part of the System including installation, testing, commissioning, operational acceptance and operations etc. in accordance with the Agreed and Finalized Project Plan and the Contract. The Progress and other reports **specified in the SCC** shall be prepared by the CSP and submitted to the Client in the format and frequency specified in the Technical Requirements.
Product Upgrades	At any point during performance of the Contract, should technological advances be introduced by the CSP for cloud and managed services originally offered by the CSP in its bid and still to be delivered, the CSP shall be obligated to offer to the Client the latest versions of the available cloud and managed services having equal or better performance or functionality at the same or lesser unit prices, pursuant to GCC Clause 0. At any point during performance of the Contract, for cloud and managed services still to be delivered, the CSP will also pass on to the Client any cost reductions and additional and/or improved support and facilities that it offers to other clients of the CSP in the Client's Country, pursuant to GCC Clause 0. During performance of the Contract, the CSP shall offer to the Client all new versions, releases, and updates of Standard Software, as well as related documentation and technical support services, within thirty (30) days of their availability from the CSP to other clients of the CSP in the Client's Country, and no later than twelve (12) months after they are released in the country of origin. In no case will the prices for these Software exceed those quoted by the CSP in the in its bid. The CSP shall provide the Client: with all new versions, releases, and updates for all Software used in the system during the Contract Period at no additional cost to the Client. The Client shall introduce all new versions, releases or updates of the Software within nine (09) months of receipt of a production-ready copy of the new version, release, or update, provided that the new version, release, or update does not adversely affect System operation or performance or require extensive reworking of the System. In cases where the new version, release, or update adversely affects System operation or performance, or requires extensive reworking of the System, the CSP shall continue to support and maintain the version or release previously in operation for as long as necessary to allow introduction of the new version, release, or update. In no case shall the CSP stop supporting or maintaining a version or release of the Software less than twenty four (24) months after the Client receives a production-ready copy of a subsequent version, release, or update. The Client shall use all reasonable endeavors to implement any new version, release, or update as soon as practicable, subject to the twenty-four-month-long stop date.
Implementation, Installation, Migration and Other Services	The CSP shall provide all Services specified in the Contract and Agreed and Finalized Project Plan in accordance with the highest standards of professional competence and integrity. Prices charged by the CSP for Services, if not included in the Contract, shall be agreed upon in advance by the parties (including, but not restricted to, any prices submitted by the CSP in its Bid) and shall not exceed the prevailing rates charged by the CSP to other Clients in the

	Client's Country for similar services.
Inspections and Tests	The Client or its representative shall have the right to inspect and/or test any components of the System remotely, as specified in the Volume III – Terms of Reference, to confirm their good working order and/or conformity to the Contract. The Client or its representative shall be entitled to review any such inspections and/or tests of the components remotely, provided that the Client shall bear all costs and expenses incurred in connection with such attendance, including but not limited to all inspection agent fees, travel, and related expenses. Should the inspected or tested components fail to conform to the Contract, the Client may reject the component(s), and the CSP shall either replace the rejected component(s), or make alterations as necessary so that it meets the Contract requirements free of cost to the Client. The Project Manager may require the CSP to carry out any inspection and/or test not specified in the Contract, provided that the CSP's reasonable costs and expenses incurred in the carrying out of such inspection and/or test shall be added to the Contract Price. Further, if such inspection and/or test impede the progress of work on the System and/or the CSP's performance of its other obligations under the Contract, due allowance will be made in respect of the Time for Achieving Operational Acceptance and the other obligations so affected. If any dispute shall arise between the Parties in connection with or caused by an inspection and/or with regard to any component to be incorporated in the System that cannot be settled amicably between the Parties within a reasonable period of time, either Party may invoke the process pursuant to GCC Clause 0 (Settlement of Disputes), starting with referral of the matter to the Adjudicator in case an Adjudicator is included and named in the Contract Agreement. *Client may employ qualified inspectors to inspect and certify the cloud and managed services provided by CSP. If such a test is required, the expenses of the trip for the Inspectors shall be borne by the CSP.*
Installation of the System	As soon as the System, or any Subsystem, has, in the opinion of the CSP, been delivered, Pre-commissioned, and made ready for Commissioning and Operational Acceptance Testing in accordance with the Volume III – Terms of Reference, the SCC and the Agreed and Finalized Project Plan, the CSP shall so notify the Client in writing. The Project Manager shall, within fourteen (14) days after receipt of the CSP's notice under GCC Clause 0, either issue an Installation Certificate, stating that the System, or major component or Subsystem (if Acceptance by major component or Subsystem is specified pursuant to the SCC for GCC Clause 0), has achieved Installation by the date of the CSP's notice under GCC Clause 0, or notify the CSP in writing of any defects and/or deficiencies, including, but not limited to, defects or deficiencies in the interoperability or integration of the various components and/or Subsystems making up the System. The CSP shall use all reasonable endeavours to promptly remedy any defect and/or deficiencies that the Project Manager has notified the CSP of. The CSP shall then promptly carry out retesting of the System or Subsystem and, when in the CSP's opinion the System or Subsystem is ready for Commissioning and

	Operational Acceptance Testing, notify the Client in writing, in accordance with GCC Clause 0. The procedure set out in this GCC Clause 0 shall be repeated, as necessary, until an Installation Certificate is issued. If the Project Manager fails to issue the Installation Certificate and fails to inform the CSP of any defects and/or deficiencies within fourteen (14) days after receipt of the CSP's notice under GCC Clause 0, or if the Client puts the System or a Subsystem into production operation, then the System (or Subsystem) shall be deemed to have achieved successful Installation as of the date of the CSP's notice or repeated notice, or when the Client put the System into production operation, as the case may be.
Commissioning and Operational Acceptance	Commissioning Commissioning of the System (or Subsystem if specified pursuant to the SCC for GCC Clause 0) shall be commenced by the CSP: immediately after the Installation Certificate is issued by the Project Manager, pursuant to GCC Clause 0; or as otherwise specified in the Terms of Reference or the Agreed and Finalized Project Plan; or immediately after Installation is deemed to have occurred, under GCC Clause 0. The Client shall supply the operating and technical personnel and all materials and information reasonably required to enable the CSP to carry out its obligations with respect to Commissioning; Production use of the System or Subsystem(s) shall not commence prior to the start of formal Operational Acceptance Testing. Operational Acceptance Tests The Operational Acceptance Tests (and repeats of such tests) shall be the primary responsibility of the Client (in accordance with GCC Clause 0), but shall be conducted with the full cooperation of the CSP during Commissioning of the System (or major components or Subsystem[s] if **specified in the SCC** and supported by the Terms of Reference), to ascertain whether the System (or major component or Subsystem[s]) conforms to the Terms of Reference and meets the standard of performance quoted in the CSP's bid, including, but not restricted to, the functional and technical performance requirements.; At the Client's discretion, Operational Acceptance Tests may also be performed on replacement Goods (if any), upgrades and new version releases, and Goods that are added or field-modified after Operational Acceptance of the System. If for reasons attributable to the Client, the Operational Acceptance Test of the System (or Subsystem[s] or major components, pursuant to the SCC for GCC Clause 0) cannot be successfully completed within the period **specified in the SCC,** from the date of Installation or any other period agreed upon in writing by the Client and the CSP, the CSP shall be deemed to have fulfilled its obligations with respect to the technical and functional aspects of the Terms of Reference, SCC and/or the Agreed and Finalized Project Plan, and GCC Clause 0 and 0 shall not apply. Operational Acceptance

	Operational Acceptance shall occur in respect of the System, when: the Operational Acceptance Tests, as specified in the Terms of Reference, and/or SCC and/or the Agreed and Finalized Project Plan have been successfully completed; or the Operational Acceptance Tests have not been successfully completed or have not been carried out for reasons that are attributable to the Client within the period from the date of Installation or any other agreed-upon period as specified in GCC Clause 0 above; or the Client has put the System into production or use for sixty (60) consecutive days. If the System is put into production or use in this manner, the CSP shall notify the Client and document such use. At any time after any of the events set out in GCC Clause 0 have occurred, the CSP may give a notice to the Client's Project Manager requesting the issue of an Operational Acceptance Certificate; After consultation with the Client, and within fourteen (14) days after receipt of the CSP's notice, the Client's Project Manager shall: issue an Operational Acceptance Certificate; or notify the CSP in writing of any defect or deficiencies or other reason for the failure of the Operational Acceptance Tests; or issue the Operational Acceptance Certificate, if the situation covered by GCC Clause 0 0 arises. The CSP shall use all reasonable endeavours to promptly remedy any defect and/or deficiencies and/or other reasons for the failure of the Operational Acceptance Test that the Project Manager has notified the CSP of. Once such remedies have been made by the CSP, the CSP shall notify the Client, and the Client, with the full cooperation of the CSP, shall use all reasonable endeavours to promptly carry out retesting of the System or Subsystem. Upon the successful conclusion of the Operational Acceptance Tests, the CSP shall notify the Client of its request for Operational Acceptance Certification, in accordance with GCC Clause 0. The Client shall then issue to the CSP the Operational Acceptance Certification in accordance with GCC Clause 00, or shall notify the CSP of further defects, deficiencies, or other reasons for the failure of the Operational Acceptance Test. The procedure set out in this GCC Clause 0 shall be repeated, as necessary, until an Operational Acceptance Certificate is issued; If the System or Subsystem fails to pass the Operational Acceptance Test(s) in accordance with GCC Clause 0, then either: the Client may consider terminating the Contract, pursuant to GCC Clause 0 0; or if the failure to achieve Operational Acceptance within the specified time period is a result of the failure of the Client to fulfill its obligations under the Contract, then the CSP shall be deemed to have fulfilled its obligations with respect to the relevant technical and functional aspects of the Contract. If within fourteen (14) days after receipt of the CSP's notice the Project Manager fails to issue the Operational Acceptance Certificate or fails to inform the CSP in writing of the justifiable reasons why the Project

	Manager has not issued the Operational Acceptance Certificate, the System or Subsystem shall be deemed to have been accepted as of the date of the CSP's said notice.

J. GUARANTEES AND LIABILITIES

Operational Acceptance Time Guarantee	The CSP guarantees that it shall complete the Installation, Integration, Commissioning, and achieve Operational Acceptance of the System (or Subsystems, pursuant to the SCC for GCC Clause 0) within the time periods specified in the Implementation Schedule in the Terms of Reference Section and/or the Agreed and Finalized Project Plan pursuant to GCC Clause 0, or within such extended time to which the CSP shall be entitled under GCC Clause 0 (Extension of Time for Achieving Operational Acceptance). If the CSP fails to install, commission, and achieve Operational Acceptance of the System (or Subsystems pursuant to the SCC for GCC Clause 0) within the time for achieving Operational Acceptance specified in the Implementation Schedule in the Terms of Reference or the Agreed and Finalized Project Plan, or any extension of the time for achieving Operational Acceptance previously granted under GCC Clause 0 (Extension of Time for Achieving Operational Acceptance), the CSP shall pay to the Client liquidated damages at the rate **specified in the SCC** as a percentage of the Contract Price, or the relevant part of the Contract Price if a Subsystem has not achieved Operational Acceptance. The aggregate amount of such liquidated damages shall in no event exceed the amount specified in the SCC ("the Maximum"). Once the Maximum is reached, the Client may consider termination of the Contract, pursuant to GCC Clause 0 0. Unless otherwise **specified in the SCC,** liquidated damages payable under GCC Clause 0 shall apply only to the failure to achieve Operational Acceptance of the System as specified in the Implementation Schedule in the Terms of Reference and/or Agreed and Finalized Project Plan. This Clause 0 shall not limit, however, any other rights or remedies the Client may have under the Contract for other delays. If liquidated damages are claimed by the Client for the System (or Subsystem), the CSP shall have no further liability whatsoever to the Client in respect to the Operational Acceptance time guarantee for the System (or Subsystem). However, the payment of liquidated damages shall not in any way relieve the CSP from any of its obligations to complete the System or from any other of its obligations and liabilities under the Contract.
Extension of Time for Achieving Operational Acceptance	The time(s) for achieving Operational Acceptance specified in the Schedule of Implementation shall be extended if the CSP is delayed or impeded in the performance of any of its obligations under the Contract by reason of any of the following: Any Change in the System as provided in GCC Clause 0 (Change in the System); Any occurrence of Force Majeure as provided in GCC Clause 0 (Force Majeure); Default of the Client; or Any other matter specifically mentioned in the Contract.

	By such period as shall be fair and reasonable in all the circumstances and as shall fairly reflect the delay or impediment sustained by the CSP. Except where otherwise specifically provided in the Contract, the CSP shall submit to the Project Manager a notice of a claim for an extension of the time for achieving Operational Acceptance, together with particulars of the event or circumstance justifying such extension as soon as reasonably practicable after the commencement of such event or circumstance. As soon as reasonably practicable after receipt of such notice and supporting particulars of the claim, the Client and the CSP shall agree upon the period of such extension. In the event that the CSP does not accept the Client's estimate of a fair and reasonable time extension, the CSP shall be entitled to refer the matter to the provisions for the Settlement of Disputes pursuant to GCC Clause 0. The CSP shall at all times use its reasonable efforts to minimize any delay in the performance of its obligations under the Contract.
Functional Guarantees	The CSP guarantees that, once the Operational Acceptance Certificate(s) has been issued, the System represents a complete, integrated solution to the Client's requirements set forth in the Terms of Reference and it conforms to all other aspects of the Contract. The CSP acknowledges that GCC Clause 0 regarding Commissioning and Operational Acceptance governs how technical conformance of the System to the Contract requirements will be determined. If, for reasons attributable to the CSP, the System does not conform to the Terms of Reference or does not conform to all other aspects of the Contract, the CSP shall at its cost and expense make such changes, modifications, and/or additions to the System as may be necessary to conform to the Terms of Reference and meet all functional and performance standards. The CSP shall notify the Client upon completion of the necessary changes, modifications, and/or additions and shall request the Client to repeat the Operational Acceptance Tests until the System achieves Operational Acceptance. If the System (or Subsystem[s]) fails to achieve Operational Acceptance, the Client may consider termination of the Contract, pursuant to GCC Clause 0 0, and forfeiture of the CSP's Performance Security in accordance with GCC Clause 0 0 in compensation for the extra costs and delays likely to result from this failure.
Intellectual Property Rights Warranty	The CSP hereby represents and warrants that: the System as supplied, installed, tested, and accepted; use of the System in accordance with the Contract; and copying of the Software and Materials provided to the Client in accordance with the Contract. Do not and will not infringe any Intellectual Property Rights held by any third party and that it has all necessary rights or at its sole expense shall have secured in writing all transfers of rights and other consents necessary to make the assignments, licenses, and other transfers of Intellectual Property Rights and the warranties set forth in the Contract, and for the Client to own or exercise all Intellectual Property Rights as provided in the Contract. Without limitation, the CSP shall secure all necessary written agreements, consents, and transfers of rights from its employees and other persons or entities whose services are used for

	development of the System.
Intellectual Property Rights Indemnity	The CSP shall indemnify and hold harmless the Client and its employees and officers from and against any and all losses, liabilities, and costs (including losses, liabilities, and costs incurred in defending a claim alleging such a liability), that the Client or its employees or officers may suffer as a result of any infringement or alleged infringement of any Intellectual Property Rights by reason of: installation of the System by the CSP or the use of the System, including any Materials, in the country where the site is located; copying of the Software and Materials provided the CSP in accordance with the Agreement; and sale of the products produced by the System in any country, except to the extent that such losses, liabilities, and costs arise as a result of the Client's breach of GCC Clause 0. Such indemnity shall not cover any use of the System, including the Materials, other than for the purpose indicated by or to be reasonably inferred from the Contract, any infringement resulting from the use of the System, or any products of the System produced thereby in association or combination with any other goods or services not supplied by the CSP, where the infringement arises because of such association or combination and not because of use of the System in its own right. Such indemnities shall also not apply if any claim of infringement: is asserted by a parent, subsidiary, or affiliate of the Client's organization; is a direct result of a design mandated by the Client's Terms of Reference and the possibility of such infringement was duly noted in the CSP's Bid; or results from the alteration of the System, including the Materials, by the Client or any persons other than the CSP or a person authorized by the CSP. If any proceedings are brought or any claim is made against the Client arising out of the matters referred to in GCC Clause 0, the Client shall promptly give the CSP notice of such proceedings or claims, and the CSP may at its own expense and in the Client's name conduct such proceedings or claim and any negotiations for the settlement of any such proceedings or claim. If the CSP fails to notify the Client within twenty-eight (28) days after receipt of such notice that it intends to conduct any such proceedings or claim, then the Client shall be free to conduct the same on its own behalf. Unless the CSP has so failed to notify the Client within the twenty-eight (28) days, the Client shall make no admission that may be prejudicial to the defense of any such proceedings or claim. The Client shall, at the CSP's request, afford all available assistance to the CSP in conducting such proceedings or claim and shall be reimbursed by the CSP for all reasonable expenses incurred in so doing. The Client shall indemnify and hold harmless the CSP and its employees, officers, from and against any and all losses, liabilities, and costs (including losses, liabilities, and costs incurred in defending a claim alleging such a liability) that the CSP or its employees, officers, may suffer as a result of any infringement or alleged infringement of any Intellectual Property Rights arising out of or in connection with any design, data,

	specification, or other documents or materials provided to the CSP in connection with this Contract by the Client or any persons (other than the CSP) contracted by the Client, except to the extent that such losses, liabilities, and costs arise as a result of the CSP's breach of GCC Clause 0. Such indemnity shall not cover: any use of the design, data, specification, or other documents or materials, other than for the purpose indicated by or to be reasonably inferred from the Contract; any infringement resulting from the use of the design, data, specification, or other documents or materials, or any products produced thereby, in association or combination with any other Goods or Services not provided by the Client or any other person contracted by the Client, where the infringement arises because of such association or combination and not because of the use of the design, data, drawing, specification, or other documents or materials in its own right. Such indemnities shall also not apply: if any claim of infringement is asserted by a parent, subsidiary, or affiliate of the CSP's organization; to the extent that any claim of infringement is caused by the alteration, by the CSP, or any persons contracted by the CSP, of the design, data, specification, or other documents or materials provided to the CSP by the Client or any persons contracted by the Client. If any proceedings are brought or any claim is made against the CSP arising out of the matters referred to in GCC Clause 0, the CSP shall promptly give the Client notice of such proceedings or claims, and the Client may at its own expense and in the CSP's name conduct such proceedings or claim and any negotiations for the settlement of any such proceedings or claim. If the Client fails to notify the CSP within twenty-eight (28) days after receipt of such notice that it intends to conduct any such proceedings or claim, then the CSP shall be free to conduct the same on its own behalf. Unless the Client has so failed to notify the CSP within the twenty-eight (28) days, the CSP shall make no admission that may be prejudicial to the defense of any such proceedings or claim. The CSP shall, at the Client's request, afford all available assistance to the Client in conducting such proceedings or claim and shall be reimbursed by the Client for all reasonable expenses incurred in so doing.
Limitation of Liability	Provided the following does not exclude or limit any liabilities of either Party in ways not permitted by applicable law: the CSP shall not be liable to the Client, whether in contract, tort, or otherwise, for any indirect or consequential loss or damage, loss of use, loss of production, or loss of profits or interest costs, provided that this exclusion shall not apply to any obligation of the CSP to pay liquidated damages to the Client; and the aggregate liability of the CSP to the Client, whether under the Contract, in tort or otherwise, shall not exceed the total cost of Performance Security required as part of the RFP, provided that this limitation shall not apply to any obligation of the CSP to indemnify the Client with respect to intellectual property rights infringement.

K. RISK DISTRIBUTION

Transfer of Ownership	With the exception of Software and Materials, the ownership of the System and other Goods shall be transferred to the Client under terms that may be agreed upon and specified in the Contract Agreement. Ownership and the terms of usage of the Software and Materials supplied under the Contract shall be governed by GCC Clause 0 (Copyright) and any elaboration in the Terms of Reference. Ownership of the CSP's Equipment used by the CSP in connection with the Contract shall remain with the CSP. Client shall retain access to all virtual machines, templates, clones, and scripts/applications created for various applications, any user created/loaded data and applications hosted on CSP's infrastructure and maintains the right to request (or shall be able to retrieve) full copies of these virtual machines at any time during the course of the Contract.
Loss of or Damage to Property; Accident or Injury to Workers; Indemnification	The CSP shall abide by the job safety, insurance, customs, and immigration measures prevalent and laws in force in the Client's Country. Subject to GCC Clause 0, the CSP shall indemnify and hold harmless the Client and its employees and officers from and against any and all losses, liabilities and costs (including losses, liabilities, and costs incurred in defending a claim alleging such a liability) that the Client or its employees or officers may suffer as a result of the death or injury of any person or loss of or damage to any property (other than the System, whether accepted or not) arising in connection with the supply, installation, testing, and Commissioning of the System and by reason of the negligence of the CSP, or their employees, officers or agents, except any injury, death, or property damage caused by the negligence of the Client, its contractors, employees, officers, or agents. If any proceedings are brought or any claim is made against the Client that might subject the CSP to liability under GCC Clause 0, the Client shall promptly give the CSP notice of such proceedings or claims, and the CSP may at its own expense and in the Client's name conduct such proceedings or claim and any negotiations for the settlement of any such proceedings or claim. If the CSP fails to notify the Client within twenty-eight (28) days after receipt of such notice that it intends to conduct any such proceedings or claim, then the Client shall be free to conduct the same on its own behalf. Unless the CSP has so failed to notify the Client within the twenty-eight (28) day period, the Client shall make no admission that may be prejudicial to the defense of any such proceedings or claim. The Client shall, at the CSP's request, afford all available assistance to the CSP in conducting such proceedings or claim and shall be reimbursed by the CSP for all reasonable expenses incurred in so doing. The Client shall indemnify and hold harmless the CSP and its employees, officers from any and all losses, liabilities, and costs (including losses, liabilities, and costs incurred in defending a claim alleging such a liability) that the CSP or its employees, officers may suffer as a result of the death or personal injury of any person or loss of or damage to property of the Client, other than the System not yet achieving Operational Acceptance, that is caused by fire, explosion, or any other perils, in excess of the

	amount recoverable from insurances procured under GCC Clause 0 (Insurances), provided that such fire, explosion, or other perils were not caused by any act or failure of the CSP. If any proceedings are brought or any claim is made against the CSP that might subject the Client to liability under GCC Clause 0, the CSP shall promptly give the Client notice of such proceedings or claims, and the Client may at its own expense and in the CSP's name conduct such proceedings or claim and any negotiations for the settlement of any such proceedings or claim. If the Client fails to notify the CSP within twenty-eight (28) days after receipt of such notice that it intends to conduct any such proceedings or claim, then the CSP shall be free to conduct the same on its own behalf. Unless the Client has so failed to notify the CSP within the twenty-eight (28) days, the CSP shall make no admission that may be prejudicial to the defense of any such proceedings or claim. The CSP shall, at the Client's request, afford all available assistance to the Client in conducting such proceedings or claim and shall be reimbursed by the Client for all reasonable expenses incurred in so doing. The party entitled to the benefit of an indemnity under this GCC Clause 0 shall take all reasonable measures to mitigate any loss or damage that has occurred. If the party fails to take such measures, the other party's liabilities shall be correspondingly reduced.
Force Majeure	"Force Majeure" shall mean any event beyond the reasonable control of the Client or of the CSP, as the case may be, and which is unavoidable notwithstanding the reasonable care of the party affected and shall include, without limitation, the following: War, hostilities, or warlike operations (whether a state of war be declared or not), invasion, act of foreign enemy, and civil war; Rebellion, revolution, insurrection, mutiny, usurpation of civil or military government, conspiracy, riot, civil commotion, and terrorist acts; Confiscation, nationalization, mobilization, commandeering or requisition by or under the order of any government or de jure or de facto authority or ruler, or any other act or failure to act of any local state or national government authority; Strike, sabotage, lockout, embargo, import restriction, port congestion, shipwreck, shortage or restriction of power supply, epidemics, quarantine, and plague; Earthquake, landslide, volcanic activity, fire, flood or inundation, tidal wave, typhoon or cyclone, hurricane, storm, lightning, or other inclement weather condition, nuclear and pressure waves, or other natural or physical disaster; Failure, by the CSP, to obtain the necessary export permit(s) from the governments of the Country(s) of Origin of the Cloud and Managed Services or other Goods, or CSP's Equipment provided that the CSP has made all reasonable efforts to obtain the required export permit(s), including the exercise of due diligence in determining the eligibility of the System and all of its components for receipt of the necessary export permits. If either Party is prevented, hindered, or delayed from or in performing any of its obligations under the Contract by an event of Force Majeure, then it shall notify the other in writing of the occurrence of such event and the circumstances of the event of Force Majeure within fourteen (14) days

	after the occurrence of such event. The Party who has given such notice shall be excused from the performance or punctual performance of its obligations under the Contract for so long as the relevant event of Force Majeure continues and to the extent that such Party's performance is prevented, hindered, or delayed. The Time for Achieving Operational Acceptance shall be extended in accordance with GCC Clause 0 (Extension of Time for Achieving Operational Acceptance). The Party or Parties affected by the event of Force Majeure shall use reasonable efforts to mitigate the effect of the event of Force Majeure upon its or their performance of the Contract and to fulfil its or their obligations under the Contract, but without prejudice to either Party's right to terminate the Contract under GCC Clause 0. No delay or non-performance by either party to this Contract caused by the occurrence of any event of Force Majeure shall: constitute a default or breach of the Contract; (subject to GCC Clauses, 0, and 0) give rise to any claim for damages or additional cost or expense occasioned by the delay or nonperformance. If, and to the extent that, such delay or non-performance is caused by the occurrence of an event of Force Majeure. If the performance of the Contract is substantially prevented, hindered, or delayed for a single period of more than sixty (60) days or an aggregate period of more than one hundred and twenty (120) days on account of one or more events of Force Majeure during the time period covered by the Contract, the Parties will attempt to develop a mutually satisfactory solution, failing which, either party may terminate the Contract by giving a notice to the other. In the event of termination pursuant to GCC Clause 0, the rights and obligations of the Client and the CSP shall be as specified in GCC Clauses 0 0 and 0. Notwithstanding GCC Clause 0, Force Majeure shall not apply to any obligation of the Client to make payments to the CSP under this Contract.

L. FAIRNESS AND GOOD FAITH

Good Faith	The Parties undertake to act in good faith with respect to each other's rights under this Contract and to adopt all reasonable measures to ensure the realization of the objectives of this Contract.

M. MISCELLANEOUS

Amicable Settlement	The Parties shall seek to resolve any dispute amicably by mutual consultation. If either Party objects to any action or inaction of the other Party, the objecting Party may send a written notice of dispute to the other Party providing in detail the basis of the dispute. The Party receiving the notice of dispute will consider it and respond in writing within fourteen (14) days after receipt. If such Party fails to respond within fourteen (14) days, or the dispute cannot be amicably settled within fourteen (14) days following the response of that Party, GCC Clause 0 shall apply.

Performance Security	The CSP shall furnish to the Client the Performance Security in the format set out in Appendix A, from a scheduled commercial bank in India, to secure the performance of its obligations under the Contract. The Performance Security shall be for an amount specified in the SCC.
Assignment	Except as expressly permitted in the Contract, the CSP shall not be entitled to divest, transfer, assign or novate all or substantially all of its rights, interests, benefits and obligations under the Contract, without the prior written consent of the Client. The Client shall be entitled to assign, transfer or novate its rights and obligations under the Contract or any part thereof to any third party or to an affiliate, without the requirement of any further consent from the CSP, provided that where such assignment is made to a third party, the Client shall use its best efforts to ensure that the third party to whom the benefits and obligations under the Contract or any part thereof has been assigned, has the necessary financial capability to comply with the obligations under the Contract.
Representation and Warranties	<u>Client's Representations and Warranties</u> The Client makes the following representations and warranties to the CSP: It has been incorporated as a company under the laws of India and is validly existing under those laws; It has power to enter into this Contract and comply with its obligations under it; This Contract and the transactions under it do not contravene its constituent documents or any Applicable Law or obligation by which it is bound or to which any of its assets are subject or cause a limitation of powers or the powers of its directors to be exceeded; It has in full force and effect the authorizations necessary for it to enter into this Contract and the transactions under it; and Its obligations under this Contract are valid and binding and are enforceable against it in accordance with the terms of this Contract. <u>CSP's Representations and Warranties</u> The CSP makes the following representations and warranties to the Client: It has been incorporated/registered as a company/firm under the laws of India and is validly existing under those laws; It has power to enter into this Contract and comply with its obligations under it; This Contract and the transactions under it do not contravene its constituent documents or any applicable law of its jurisdiction or obligation by which it is bound or to which any of its assets are subject or cause a limitation of powers or the powers of its directors to be exceeded; It has in full force and effect the authorizations necessary for it to enter into this Contract and the transactions under it; Its obligations under this Contract are valid and binding and are enforceable against it in accordance with the terms of this Contract;

	It is not in breach of any Applicable Law in a way which may result in a material adverse effect on its business or financial condition; There is no pending or threatened proceeding affecting the CSP or any of its assets that would affect the validity or enforceability of this Contract, the ability of the CSP to fulfil its commitments under this Contract, or that could have a material adverse effect on the business or financial condition of the CSP; It has not been subject to any fines, penalties, injunctive relief or any other civil or criminal liabilities which in the aggregate have or may have a material adverse effect on its ability to perform its obligations under the Contract; It has the necessary skill and experience to perform the Services in accordance with this Contract; It owns or has the right to use and license to the Client all Intellectual Property Rights in relation to the Services and the Deliverables to be provided under this Contract; The performance of the Services shall not infringe the Intellectual Property Rights of any third party and that the CSP has not received notice of any claim, and is not aware of any facts or circumstances that may give rise to such claim; It will perform its obligations under the Contract and conduct its business with a high level of integrity which is reasonably expected of an international contractor of similar size and profile, conducting a similar line of business, and will not engage in any corrupt, fraudulent, coercive, collusive, undesirable or restrictive practices; and Without prejudice to any express provision contained in the Contract, the CSP acknowledges that prior to the execution of the Contract, the CSP has after a complete and careful examination made an independent evaluation of the Technical Requirements and any information provided by or on behalf of the Client and has determined to its satisfaction the nature and extent of risks and hazards as are likely to arise or may be faced by the CSP in the course of performance of its obligations hereunder.
Other Miscellaneous Stipulations	Client shall pay for cloud and managed services quarterly based on Client's actual consumption of cloud resources on the basis of pay you per use model without any minimum charges; Unit rate mentioned as part of the financial proposal (Financial Proposal Submission Forms – Recurring Costs – Form 1.5) shall be followed for Pay as per Use model and shall be applicable for entire duration of the Contract. Requirements presented as part of Financial Proposal is indicative and is for the purpose of price discovery only. No commercial commitment shall be assumed by the CSP based on the Financial Proposal. Financial proposal (Recurring Costs – Form 1.5) is to discover unit process so that the Client can pay as per pay-as-per-use model during consumption of cloud and managed services; If in case Client requires additional systems which are not a part of existing line items in (Financial Proposal Submission Forms – Recurring Costs – Form 1.5), then Client shall procure the systems as per the rate card provided as part of (Financial Proposal Submission Forms– Form 1.7..

	DRC / Secondary DC as a Service can be opted by the Client at later stage based on Client's discretion. The unit rates offered as part of Financial Proposal (Financial Proposal Submission Forms – DRC / Secondary DC Costs – Form 1.6) shall be applicable (as per Client's discretion) in case DRC / Secondary DC as a Service is required.

Attachment 1: Corrupt and Fraudulent Practices

1. The CSPs and their respective officers, employees, agents and advisers shall observe the highest standard of ethics during the selection process. Notwithstanding anything to the contrary contained in the RFP, the Client shall reject a Proposal without being liable in any manner whatsoever to the CSP, if it determines that the CSP has, directly or indirectly or through an agent, engaged in corrupt practice, fraudulent practice, coercive practice, undesirable practice or restrictive practice (collectively the "Prohibited Practices") in the selection process. In such an event, the Client shall, without prejudice to its any other rights or remedies, forfeit and appropriate the Performance Security, if available, as mutually agreed genuine pre-estimated compensation and damages payable to the Client for, *inter alia,* time, cost and effort of the Client, in regard to the RFP, including consideration and evaluation of such CSP's Proposal.

2. Without prejudice to the rights of the Client under the RFP and the rights and remedies which the Client may have under the LOA or the Contract, if an CSP is found by the Client to have directly or indirectly or through an agent, engaged or indulged in any corrupt practice, fraudulent practice, coercive practice, undesirable practice or restrictive practice during the selection process, or after the issue of the LOA or the execution of the Contract, such Applicant or CSP shall not be eligible to participate in any tender or RFP issued by the Client during a period of 2 (two) years from the date such CSP is found by the Client to have directly or through an agent, engaged or indulged in any corrupt practice, fraudulent practice, coercive practice, undesirable practice or restrictive practice, as the case may be.

3. For the purposes of this clause, the following terms shall have the meaning hereinafter respectively assigned to them:

    5. "corrupt practice" means (a) the offering, giving, receiving, or soliciting, directly or indirectly, of anything of value to influence the action of any person connected with the selection process (for avoidance of doubt, offering of employment to or employing or engaging in any manner whatsoever, directly or indirectly, any official of the Client who is or has been associated in any manner, directly or indirectly with the selection process) or the LOA or has dealt with matters concerning the Contract or arising therefrom, before or after the execution thereof, at any time prior to the expiry of one year from the date such official resigns or retires from or otherwise ceases to be in the service of the Client, shall be deemed to constitute influencing the actions of a person connected with the selection process; or (b) save as provided herein, engaging in any manner whatsoever, whether during the selection process or after the issue of the LOA or after the execution of the Agreement, as the case may be, any person in respect of any matter relating to the Services or the LOA or the Contract, who at any time has been or is a legal, financial or technical CSP/ adviser of the Client in relation to any matter concerning the Contract;

    6. "fraudulent practice" means a misrepresentation or omission of facts or disclosure of incomplete facts, in order to influence the selection process;

    7. "coercive practice" means impairing or harming or threatening to impair or harm, directly or indirectly, any persons or property to influence any person's participation or action in the selection process;

    8. "collusive practices" is an arrangement between two or more parties designed to achieve an improper purpose, including to influence improperly the actions of another party[1];

    9. "undesirable practice" means (a) establishing contact with any person connected with

or employed or engaged by the Client with the objective of canvassing, lobbying or in any manner influencing or attempting to influence the selection process; or (b) having a Conflict of Interest; and

10. "restrictive practice" means forming a cartel or arriving at any understanding or arrangement among CSPs with the objective of restricting or manipulating a full and fair competition in the selection process.

1. Special Conditions of Contract

[Notes in brackets are for guidance purposes only and should be deleted in the final text of the signed contract]

Number of GCC Clause	**Amendments of, and Supplements to, Clauses in the General Conditions of Contract**
GCC 0	The Contract shall be construed in accordance with the law in the state of Maharashtra / India.
GCC 0	The language is: English.
GCC 0 and 0	The addresses are: Client : Maharashtra Industrial Township Limited (MITL) Attention : _____ Facsimile : _____ E-mail (where permitted):_____ CSP : _____ _____ Attention : _____ Facsimile : _____ E-mail (where permitted) :_____
GCC 0	The Authorized Representatives are: For the Client: [Insert name] Managing Director, Maharashtra Industrial Township Limited (MITL) _____ For the CSP: *[name, title]*_____
GCC 0	**Commencement of Contract:**

	On or Before "Effective Date"
GCC 0	**Expiration of Contract:** The term of the Contract shall be Twenty-Six (26) months, which may be extended on mutually agreed terms and conditions possibly for Twenty-Four (24) months subject to satisfactory performance of the Services by the CSP. If the term of the Contract is extended pursuant to the Clause 0 of the GCC, then the CSP shall also extend the validity of the Performance Security for an equivalent period. Upon such extensions, terms and conditions as per GCC clause 0 shall be applicable.
GCC 00	*The CSP shall obtain Third-Party Liability Insurance in the amount of INR 25 Lakhs. The Insurance shall cover the entire Contract Period.*
GCC 00	*Professional Liability Insurance: CSP will maintain at its expense, Professional Liability Insurance including coverage for errors and omissions caused by CSP's negligence, breach in the performance of its duties under this Contract from an Insurance Company permitted to offer such policies in India, for the entire Contract duration, (i) For an amount equal to INR Twenty Five Lakhs (INR 25,00,000) (ii) the proceeds, the CSP may be entitled to receive from any insurance maintained by the CSP to cover such a liability, whichever of (i) or (ii) is higher with a minimum coverage of [insert amount and currency]. The indemnity limit in terms of "Any One Accident" (AOA) and "Aggregate limit on the policy period" (AOP) should not be less than the amount stated in the contract. The insurance shall cover the entire contract period commencing from the date of the signing of the contract till the effective date of the expiry of the contract.* *The CSP shall maintain standard forms of comprehensive insurance including liability insurance, system and facility insurance and any other insurance for the personnel, assets, data, software, etc.* *The certificates of insurance shall indicate that the insurance company will notify the Client if, for any reason, the insurance coverage lapses.*
GCC 0	*The **CSP** shall commence work on the System as per "Effective Date"*
GCC 0	*Operational Acceptance will occur as per Implementation Plan provided in Terms of Reference and/or Approved and Finalized Project Plan. .*
GCC 000	The Performance Security shall be denominated in the currency of the contract for an amount equal to 10% of the contract value (Grand Total/Evaluated Bid Price (C) as per Form 1.3 of Financial Proposal) including taxes in INR.
GCC 0	Subject to the provisions of GCC Clause 0, the Client shall pay the Contract Price to the CSP according to the categories and in the manner specified below. The Total Contract Price shall be categorized as: • One Time Costs : This includes all one-time costs up to the

Operational Acceptance;

- Recurring Costs: This includes all quarterly payments during operations and support phase.

One Time Costs:

Milestone	Payment
One time cost of setting up cloud infrastructure for all the scope applications for pre-production an production environments	As per CSP's quote in the financial proposal for the respective milestone
Migration Services for existing Applications	As per CSP's quote in the financial proposal for the respective milestone
Any other One-Time Costs with description	As per CSP's quote in the financial proposal for the respective milestone

All payments shall be upon completion and sign-off received from the Client for the respective milestones.

Recurring Costs:

Recurring costs during the Operations Period – Shall be paid quarterly on the basis of Pay as per Use model where unit prices as specified in the Financial Proposal shall prevail during the Contract. There shall be no minimum charges by the CSP. Payment shall be made as per following:

2. For all machine associated consumption, payment shall be made on per hour basis.
3. For all storage related consumption, payment shall be made on per GB basis.
4. For all bandwidth related consumption, lump sum cost per 100 Mbps port per quarter has been submitted by CSP as part of its Financial Proposal. All quarterly payments shall be made on the lump sum quote provided.
5. For 'Other Solution', lump sum cost for every quarter has been submitted by CSP as part of its financial proposal. All quarterly payments shall be made on the same lump sum quote provided.

Quarterly payments shall be paid after deductions of any penalty arising out of service level agreement.

Terms and conditions in accordance to GCC Clause 0 shall be applicable for payments.

All payments to be made upon respective approval by MITL and its representatives and upon deployment of the Cloud infrastructure by the Client.

GCC 0	Payments shall be done in below account of the CSP: *[insert account details viz.,* *1. account name;* 2. *account number;* 3. *bank name and branch; and* 4. *IFSC Code]*
GCC 0	*The Client's and CSP's rights and obligations with respect to Custom Software or elements of the Custom Software, if any, are as follows :* *1. The CSP shall hand over the source code for software, database, and executables to the Client which shall correspond 100% to the operational module and shall be verified and certified by an independent agency as identified by the Client. This is limited to all custom software and its subsystems provided by the CSP;* **2.** *The Client may duplicate and use the software on different equipment, such as for back-ups, additional computers, replacements, upgraded units, etc.*
GCC 0	***Not Applicable.***
GCC 0	***The provisions of this GCC Clause 0 shall survive the termination, for whatever reason, of the Contract for the period specified in the GCC.***
GCC 0	***No additional powers or limitations.***
GCC 0	***No additional powers or limitations.***
GCC 0	Chapters in the Project Plan shall address the following subjects**:** ***Project Organization and Management Plan;*** ***Installation Plan;*** ***Training Plan;*** ***Pre-commissioning and Operational Acceptance Testing Plan;*** ***Operations Plan;*** ***Task, Time, and Resource Schedules;*** ***Technical Support Plan and Operations Manuals.*** ***Preventive Maintenance Plan*** ***Exit Management Plan*** ***Any other submission relevant to the project as required by the Client or its Project Manager post contract award.***

GCC 0	*Within **Seven (7) days** from the Effective Date of the Contract, the CSP shall present a Project Plan to the Client. The Client shall, within **seven (7)** days of receipt of the Project Plan, notify the CSP of any respects in which it considers that the Project Plan does not adequately ensure that the proposed program of work, proposed methods, and/or proposed cloud and managed services will satisfy the Technical Requirements and/or the SCC (in this Clause 0 called "non-conformities" below). The CSP shall, within **five (5)** days of receipt of such notification, correct the Project Plan and resubmits to the Client. The Client shall, within **five (5)** days of resubmission of the Project Plan, notify the CSP of any remaining non-conformities. This procedure shall be repeated as necessary until the Project Plan is free from non-conformities. When the Project Plan is free from non-conformities, the Client shall provide confirmation in writing to the CSP. This approved Project Plan ("the Agreed and Finalized Project Plan") shall be contractually binding on the Client and the CSP. In case of any deviation (which affects the project timelines and deliverables) from the finalized project plan during the course of the project, the CSP is required to update the same within 5 days of such deviation and notify the Client and get the approval as per the timelines mentioned above.*
GCC 0	*The CSP shall submit to the Client the following reports during the Contract period:* ***(a) Monthly progress reports, summarizing:*** ***(i) Cloud and managed services used during the month along with a dashboard view;*** ***(ii) Issues and outstanding problems; proposed actions to be taken;*** ***(iii) Breach of SLAs for the month;*** ***(iv) other issues or potential problems the CSP foresees that could impact on project progress and/or effectiveness.*** ***(b) Inspection and quality assurance reports;*** ***(c) System failure or fault reports;*** ***(d) Monthly log of service calls and problem resolutions**.* *Any other report as required by the Client which is related to the present procurement.*
GCC 0	*Operational Acceptance Testing shall be conducted in accordance with acceptance test.*
GCC 0	***Thirty (30)** days from the date of System Acceptance.*
GCC 0	*Liquidated damages shall be assessed at 1.0 percent per week of Performance Security during implementation phase. The maximum liquidated damages are 10 percent of the Performance Security during the implementation phase of the project.*

GCC 0	Performance Security: 1. The Performance Security shall be INR 10 % of the contract Value (Grand Total/Evaluated Bid Price (C) as per Form of Financial Proposal) including taxes in INR; 2. The Performance Security shall be issued by a Scheduled Commercial bank in India and acceptable to the Client. The Performance Security shall be valid until a date 60 days beyond the issuance of the Completion Certificate; 3. The Client shall not make a claim under the Performance Security, except for amounts to which the Client is entitled under the Contract in the event of: 1. failure by the CSP to extend the validity of the Performance Security on extension of the validity of the Contract, in which event the Client may claim the full amount of the Performance Security; 2. failure by the CSP to pay the Client an amount due, as either agreed or determined pursuant to the dispute resolution process specified in the Contract, within forty two (42) days after determination of the dispute; 3. failure by the CSP to pay any damages due to the Client under the Contract; 4. failure by the CSP to pay any amounts that are due to the Client on termination of the Contract; 5. the CSP engaging in any corrupt, fraudulent, coercive, collusive, undesirable or restrictive practice. 6. If the Performance Security is or becomes invalid for any reason during the term of the Contract, the CSP shall immediately notify the Client and provide the Client with a replacement Performance Security in the form set out in Appendix A within five (5) days of the earlier Performance Security becoming invalid; 7. If the validity period of the Performance Security is less than the period specified in sub-clause (ii) above, then no later than thirty (30) days before the expiry of the Performance Security, the CSP shall obtain an extension of the validity of such Performance Security and provide the Client with a copy of the renewed security. If the CSP fails to extend the Performance Security, the Client shall be entitled to draw on and claim the un-drawn amount thereunder, provided that the amount so received shall be treated as a cash security and to the extent that there are no outstanding claims, shall be released upon submission of a new Performance Security acceptable to the Client; 8. The provision, maintenance or renewal of the Performance Security by the CSP in accordance with the terms of the Contract, shall be a condition precedent to any payment by the Client to the CSP. On completion of the contractual obligations under the Contract by the CSP, the Client shall return the Performance Security within twenty-one (21) days of the last payment made to the CSP under the Contract.

13 Service Levels Agreements

13.1 Service Levels

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

13.1.1 Purpose

1. The purpose of Service Levels is to define the levels of service provided by the Cloud Service Provider ("**CSP**") to Maharashtra Industrial Township Limited ("**Client**") for the duration of the contract. The benefits of this are:

1. Help the Client control the levels and performance of CSP's services.

2. Create clear requirements for the measurement of the performance of the system and help in monitoring the same during the Contract duration.

    2. The Service Levels are between the Client and CSP.

13.1.2 Service Level Agreements & Targets

1. This section is agreed to by Client and CSP as the key performance indicator for the project.

2. The following section reflects the measurements to be used to track and report system's performance on a regular basis. The targets shown in the following tables are for the period of Contact.

13.2 General Principles of Service Level Agreements

13.2.1 Service Level Agreements

Service Level Agreement (SLA) shall become the part of the Contract between the Client and the CSP. SLA defines the terms of CSP's responsibility in ensuring the timely delivery of the services and the correctness of the services based on the agreed performance indicators as detailed in this section.

The CSP shall comply with the SLAs to ensure adherence to project quality and availability of services throughout the duration of the Contract. For the purpose of the SLA, definitions and terms as specified in the document along with the following terms shall have the meanings set forth below:

1. "Total Time" – Total number of hours in the quarter being considered for evaluation of SLA performance.

2. "Downtime" – Time period for which the specified services/components/system are not available in the concerned period, being considered for evaluation of SLA, which shall exclude downtime owing to Force Majeure and reasons beyond control of the CSP.

3. "Scheduled Maintenance Time" – Time period for which the specified services/components/system with specified technical and service standards are not available due to scheduled maintenance activity. The CSP shall seek at least 15 days prior written approval from the Client for any such activity. The scheduled maintenance shall be carried out during non-peak hours and shall not exceed more than four (4) hours and not more than four (4) times in a year.

4. "Uptime" – Time period for which the specified services are available in the period being considered for evaluation of SLA.
5. Uptime (%) = (1-{[Total Downtime] / [Total Time- Scheduled Maintenance Time]})*100. Penalties shall be applied for each criteria individually and then added together for the total penalty for a particular quarter.
6. "Incident" – Any event/abnormalities in the service/system being provided that may lead to disruption in regular/normal operations and services to the end user.
7. "Response Time" – Time elapsed from the moment an incident is reported to the Helpdesk either manually or automatically through the system to the time when a resource is assigned for the resolution of the same.
8. "Resolution Time" – Time elapsed from the moment incident is reported to the Helpdesk either manually or automatically through system, to the time by which the incident is resolved completely and services as per the Contract are restored.
9. "Target" – is the availability of cloud and managed services and their data. It is calculated as = [(Total uptime of all cloud and managed services in a quarter)/(Total time in quarter)]*100.
10. Latency: Latency may address the storage and the time when the data is placed on mirrored storage.
11. Maximum Data Restoration Time: refers to the committed time taken to restore cloud service customer data from a backup.
12. Recovery Point Objective: It is the maximum allowable time between recovery points. RPO does not specify the amount of acceptable data loss, only the acceptable time window. RPO affects data redundancy and backup.
13. Recovery Time Objective: It is the maximum amount of time a business process may be disrupted, after a disaster, without suffering unacceptable business consequences. Cloud services can be critical components of business processes.
14. Availability of Reports (Reports such as Provisioning, Utilization Monitoring Reports, User Profile Management etc.)

Penalty shall be applied for each criteria individually as per downtime of each applicable component and then added together for the total penalty for a particular quarter.

13.3 Service Levels Monitoring

The Service Level parameters shall be monitored on a quarterly basis. Penalties associated with performance for SLAs shall be made after deducting from applicable payments of the quarter or through the Performance Bank Guarantee.

As part of the Project requirements, CSP shall supply and make sure of appropriate system (software/hardware) to automate the procedure of monitoring SLAs during the course of the Contract and submit reports for all SLAs as mentioned in this section. This software along with any system specific software shall be used by the CSP for monitoring and reporting these SLAs. The Client reserves the right to test and audit these tools for accuracy and reliability at any time. If at any time during the test and audit the accuracy and reliability of tools shall be found to be compromised, the Client reserves the right to invoke up to double the penalty of the respective quarterly phase.

The CSP will endeavour to exceed these levels of service wherever possible.

CSP undertakes to notify the Client of any difficulties, or detrimental/adverse findings as soon as possible once they are identified.

CSP will provide a supplemental report on any further information received, as soon as the information becomes available.

CSP will take instruction only from authorised personnel of the Client.

In case issues are not rectified to the complete satisfaction of Client, within a reasonable period of time defined in the RFP, the Client shall have the right to take appropriate remedial actions including liquidated damages, applicable penalties, or termination of the Contract.

For issues i.e. breach of SLAs beyond control of the CSP, the CSP shall submit a justification for the consideration of the Client. In case it is established that the CSP was responsible for such breach, respective penalty shall be applied to the CSP.

13.4 Measurements & Targets

13.4.1 Operations Phase SLAs

These SLAs shall be used to evaluate the performance of the services post the Implementation Phase and during the operations Phase. These SLAs and associated performance shall be monitored on a quarterly basis. Penalty levied for non-performance as per SLA shall be deducted through subsequent payments due from the Client or through the Performance Bank Guarantee.

The Scheduled Maintenance Time shall be agreed upon with the Client as per the definition given as part of this section of the Contract.

CSP's published SLAs and penalties shall be also be applicable on the CSP during the course of the Contract. In case of any penalty is not published for any CSP's SLA, CSP shall inform the Client and the penalties will be decided by the Client based on mutual discussions with the CSP. Client and CSP shall also have an option of modifying the SLAs which are given below, as per mutual discussion, if ever there are modifications on the published SLAs of the CSP.

13.4.2 Note

Downtime calculated shall not include:

1. Down time due to hardware/software and application owned by MITL;
2. Negligence or other conduct of MITL or its agents, including a failure or malfunction resulting from applications or services provided by MITL or its System Integrators;
3. Failure or malfunction of any equipment or services not provided by the CSP.

However, it shall be the responsibility of the CSP to prove that the outage is attributable to MITL. The CSP shall obtain the proof authenticated by the MITL's official that the outage is attributable to the MITL.

13.4.3 Reporting Procedures

CSP representative shall prepare and distribute Service level performance reports in a mutually agreed format within the **first fifteen (15) days of each subsequent Quarter**. The reports shall include **"actual versus target"** Service Level Performance, a variance analysis and discussion of appropriate issues or significant events. Performance reports shall be distributed to Client management personnel as directed by Client.

Also, CSP may be required to get the Service Level performance report audited by a third-party Auditor appointed by the Client.

13.4.4 Service Level Change Control

13.4.4.1 General

It is acknowledged that this **Service levels may change as Client's business needs evolve over the course of the contract period.** As such, this document also defines the following management procedures:

4. A process for negotiating changes to the Service Levels
5. An issue management process for documenting and resolving particularly difficult issues.
6. Client and CSP management escalation process to be used in the event that an issue is not being resolved in a timely manner by the lowest possible level of management.

Any changes to the levels of service provided during the term of this Agreement shall be requested, documented and negotiated in good faith by both parties. Either party can request a change.

Service Level Change Process: The parties may amend Service Level by mutual agreement in accordance. Changes can be proposed by either party. Unresolved issues shall also be addressed. CSP's representative shall maintain and distribute current copies of the Service Level document as directed by Client. Additional copies of the current Service Levels shall be available at all times to authorized parties.

Version Control / Release Management: All negotiated changes shall require changing the version control number. As appropriate, minor changes may be accumulated for periodic release or for release when a critical threshold of change has occurred.

13.4.5 Governing Law and Dispute Resolution

Governing Law: The rights and obligations of the Parties hereunder shall be governed by, and construed in accordance with, the laws of the Republic of India.

Dispute Resolution: As per GCC and SCC

13.4.6 Notices

Form of Notice

Any notice, consent, request, demand, approval or other communication to be given or made under or in connection with the Contract (each, a "**Notice**" for the purposes of this clause) shall be in English, in writing and signed by or on behalf of the person giving it.

Address for Service

Notices shall be addressed as follows:

Notices to the CSP

Name	:	_____
Address	:	_____
Helpdesk Number	:	[Insert two different contact details for helpdesk]
Email Address	:	_____
Fax number	:	_____
To the attention of	:	Mr/Ms/Mrs _____

Notices to the Client:

Name	:	_____
Address	:	_____
Fax number	:	_____
To the attention of	:	Mr/Ms/Mrs _____

24*7 helpdesk support shall be provided by CSP on the helpdesk numbers provided above.

Change of details

A Party may change its address for service provided that it gives the other Parties not less than [•] (<insert number in words>) days' prior notice in accordance with the aforesaid. Until the end of such notice period, service on either address shall remain effective.

1. Assignment

This Agreement, or any right or interest herein, shall not be assignable or transferable by any Party except with the prior written consent of the other Parties.

2. Amendments

This Agreement may not be amended, modified or supplemented except by a written instrument executed by each of the Parties.

3. No Partnership

Nothing herein shall constitute or be construed to be or to create a partnership or joint venture or association of person between CSP and Client. The Client shall not be liable for the payment of debts, taxes, obligations or other liabilities of CSP which have been incurred by CSP in the performance of its duties. It is hereby agreed and declared that each of the Parties have undertaken obligations and has rights specified herein on their own account and on principal to principal basis and not on behalf of or on account of or as agent of any of them or of anyone else. No Party shall act as an agent of the other Party or have any authority to act for or to bind the other Party.

4. Counterparts

The Contract may be executed in one or more counterparts, each of which when so executed and delivered shall be deemed an original but all of which together shall constitute one and the same instrument and any Party may execute the Contract by signing any one or more of such originals or counterparts. The delivery of signed counterparts by facsimile transmission or electronic mail in "portable document format" (".pdf") shall be as effective as signing and delivering the counterpart in person.

14 Penalty Terms for Quality of Services

For the MITL to ensure that the Cloud Service Provider adhere to the Service Level Agreement. In case these service levels cannot be achieved at service levels defined in the agreement, the MITL will invoke the performance related penalties.

All the SLA related terms are explained in the SLA agreement. The penalty in the percentage of the Quarterly payment has been as indicated against each SLA parameter in the table.

Service Level Objective	Measurement	Target Service Level	Penalty Clause
Availability/Uptime of cloud services and Resources for CSP's Infrastructure	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, orchestration layer, virtualization layer) provisioned in the cloud. Measured with the help of SLA reports provided by CSP	<99.95% & >=99.5%	1% of Quarterly Payment
		< 99.5% & >=99%	2% of Quarterly Payment
		Subsequently, every 0.5% drop in SLA criteria	Additional 1% of Quarterly Payment till event of default and termination
Data Security, Data Privacy Incident or Data Breach, Data Mining and Management Reporting - 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. Quarter). Incident Response - CSP shall assess and acknowledge the defined incidents within 1 hour after discovery.	<95% and >=90% within 1 hour	1% of Quarterly Payment
		<90% and >=85% within 1 hour	2% of Quarterly Payment
		Subsequently, every 5% drop in SLA criteria	Additional 1% of Quarterly Payment till event of default and termination
Data Security, Data Privacy Incident or Data Breach, Data Mining and Management Reporting – Percentage of timely incident resolutions	Measured as a percentage of defined incidents against the cloud service that are resolved within a predefined time limit (quarter) over the total number of defined incidents to the cloud service within a predefined period (quarter). Measured from Incident	<95% and >=90% within 1 hour	1% of Quarterly Payment
		<90% and >=85% within 1 hour	5% of Quarterly Payment
		Subsequently, every 5% drop in SLA criteria	Additional 1% of Quarterly Payment till event of default and termination

Service Level Objective	Measurement	Target Service Level	Penalty Clause
	Reports		
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 – 30 days - Maintain 99.95% service level Medium Severity Vulnerabilities – 90 days - Maintain 99.95% service level	<99.95% and >=99	1% of Quarterly Payment
		<99% and >=98%	2% of Quarterly Payment
		Subsequently, every 1% drop in SLA criteria	Additional 2% of Quarterly Payment till event of default and termination
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% and >=99	1% of Quarterly Payment
		<99% and >=98%	2% of Quarterly Payment
		Subsequently, every 1% drop in SLA criteria	Additional 1% of Quarterly Payment till event of default and termination
Security and Privacy breach including Data Theft / Loss/ Corruption/Mining	Any incident where in system compromised, privacy breached, data is corrupted, data is mined or any case wherein data theft occurs (including internal incidents)	No breach	For each breach / data theft / data corruption / data mining issue / privacy breach, penalty will be levied as per the following criteria. Any confirmed security incident, established by root cause analysis to be attributable to an act, omission or negligence of the CSP – INR 2 Lakhs. This penalty is applicable per incident. The aggregate of all

Service Level Objective	Measurement	Target Service Level	Penalty Clause
			penalties levied under this head in any quarter shall not exceed 10% (ten percent) of the Quarterly Payment for that quarter, and shall form part of, and be counted towards, the overall SLA penalty cap per quarter. In case of serious breach of security wherein the data is stolen, mined, privacy breached or corrupted, Client reserves the right to terminate the contract.
Meeting Recovery Time Objective (RTO) (If Secondary DC / DRC as a Service is taken by the Client)	Measured during the regular planned or unplanned (outage) changeover from DC to secondary DC / DRC or vice versa.	As per project requirement given in Scope of Work. If it exceeds as per below following penalties to be levied	
		RTO – 4 hours	1% of Quarterly Payment shall be deducted
		For every increase of 30 mins in RTO	Additional 2% of Quarterly Payment till event of default and termination
Meeting Recovery Point Objective (RPO)_ (If Secondary DC / DRC as a Service is taken by the Client)	Measured during the regular planned or unplanned (outage) changeover from DC to secondary DC / DRC or vice versa	As per project requirement given in Scope of Work. If it exceeds as per below, following penalties to be levied	
		RPO – 2 hours	1% of Quarterly Payment shall be deducted
		For every increase of 30 mins in RPO	Additional 2% of Quarterly Payment till event of default and termination

Service Level Objective	Measurement	Target Service Level	Penalty Clause
Availability of the network links at DC and DR/Secondary DC (If Secondary DC / DRC as a Service is taken by the Client)	Availability (as per the definition in the SLA) will be measured for each of the network links provisioned in the cloud.	Availability for each of the network links: >= 99.5%	No Penalty
		<99.5 and => 99%	1% of quarterly payment
		<99 and => 98.5%	2% of quarterly payment
		<98.5%	3% of quarterly payment

Service Level Agreement

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

Purpose

The purpose of Service Levels is to define the levels of service provided by the Cloud Service Provider (“CSP”) to MITL (“Client”) for the duration of the contract. The benefits of this are:

Help the Client control the levels and performance of CSP’s services.

Create clear requirements for measurement of the performance of the system and help in monitoring the same during the Contract duration.

The Service Levels are between the Client and CSP.

Service Level Agreements & Targets

This section is agreed to by Client and CSP as the key performance indicator for the project.

The following section reflects the measurements to be used to track and report system’s performance on a regular basis. The targets shown in the following tables are for the period of Contact.

General Principles of Service Level Agreements

Service Level Agreement (SLA) shall become the part of the Contract between the Client and the CSP. SLA defines the terms of CSP’s responsibility in ensuring the timely delivery of the services and the correctness of the services based on the agreed performance indicators as detailed in this section.

The CSP shall comply with the SLAs to ensure adherence to project quality and availability of services throughout the duration of the Contract. For the purpose of the SLA, definitions and terms as specified in the document along with the following terms shall have the meanings set forth below:

“Total Time” – Total number of hours in the quarter being considered for evaluation of SLA performance.

“Downtime” – Time period for which the specified services/components/system are not available in the concerned period, being considered for evaluation of SLA, which shall exclude downtime owing to Force Majeure and reasons beyond control of the CSP.

“Scheduled Maintenance Time”– Time period for which the specified services/components/system with specified technical and service standards are not available due to scheduled maintenance activity. The CSP shall seek at least

15 days’ prior written approval from the Client for any such activity. The scheduled maintenance shall be carried out during non-peak hours and shall not exceed more than four (4) hours and not more than four (4) times in a year.

“Uptime” – Time period for which the specified services are available in the period being considered for evaluation of SLA.

Uptime (%) = (1- {[Total Downtime] / [Total Time- Scheduled Maintenance Time]}) * 100. Penalties shall be applied for each criterion individually and then added together for the total penalty for a particular quarter

“Incident” – Any event/abnormalities in the service/system being provided that may lead to disruption in regular/normal operations and services to the end user.

“Response Time” – Time elapsed from the moment an incident is reported to the Helpdesk either manually or automatically through the system to the time when a resource is assigned for the resolution of the same.

“Resolution Time” – Time elapsed from the moment incident is reported to the Helpdesk either manually or automatically through system, to the time by which the incident is resolved completely and services as per the Contract are restored.

“Target” – is the availability of cloud and managed services and their data. It is calculated as = [(Total uptime of all cloud and managed services in a quarter)/(Total time in quarter)]*100.

Latency: Latency may address the storage and the time when the data is placed on mirrored storage.

Maximum Data Restoration Time: refers to the committed time taken to restore cloud service customer data from a backup.

Recovery Point Objective: It is the maximum allowable time between recovery points. RPO does not specify the amount of acceptable data loss, only the acceptable time window. RPO affects data redundancy and backup.

Recovery Time Objective: It is the maximum amount of time a business process may be disrupted, after a disaster, without suffering unacceptable business consequences. Cloud services can be critical components of business processes.

Availability of Reports (Reports such as Provisioning, Utilization Monitoring Reports, User Profile Management etc.)

Penalty shall be applied for each criterion individually as per downtime of each applicable component and then added together for the total penalty for a particular quarter.

Service Levels Monitoring

The Service Level parameters shall be monitored on a quarterly basis. Penalties associated with performance for SLAs shall be made after deducting from applicable payments of the quarter or through the Performance Bank Guarantee.

As part of the Project requirements, CSP shall supply and make sure of appropriate system (software/hardware) to automate the procedure of monitoring SLAs during the course of the Contract and submit reports for all SLAs as mentioned in this section. This software along with any system specific software shall be used by the CSP for monitoring and reporting these SLAs. The Client reserves the right to test and audit these tools for accuracy and reliability at any time. If at any time during the test and audit the accuracy and reliability of tools shall be found to be compromised, the Client reserves the right to invoke up to double the penalty of the respective quarterly phase.

The CSP will endeavour to exceed these levels of service wherever possible.

CSP undertakes to notify the Client of any difficulties, or detrimental/adverse findings as soon as possible once they are identified.

CSP will provide a supplemental report on any further information received, as soon as the information becomes available.

CSP will take instruction only from authorized personnel of the Client.

In case issues are not rectified to the complete satisfaction of Client, within a reasonable period of time defined in the RFP, the Client shall have the right to take appropriate remedial actions including liquidated damages, applicable penalties, or termination of the Contract.

For issues i.e. breach of SLAs beyond control of the CSP, the CSP shall submit a justification for the consideration of the Client. In case it is established that the CSP was responsible for such breach, respective penalty shall be applied to the CSP.

Measurements & Targets - Operations Phase SLAs

These SLAs shall be used to evaluate the performance of the services post the Implementation Phase and during the operations Phase. These SLAs and associated performance shall be monitored on a quarterly basis. Penalty levied for non-performance as per SLA shall be deducted through subsequent payments due from the Client or through the Performance Bank Guarantee.

The Scheduled Maintenance Time shall be agreed upon with the Client as per the definition given as part of this section of the Contract.

CSP's published SLAs and penalties shall be also being applicable during the course of the Contract.

The following SLAs apply for CSP. While the CSP will be responsible for maintaining the SLAs pertaining to the cloud infrastructure, network, controls etc., the CSP will be responsible for the SLAs related to managing and monitoring the cloud services.

Sr.no	Parameter	Metric	Penalty
1	Database Server Uptime Application Server Uptime Web Server Uptime SAN Storage Uptime Internet Link Any other IT component in the Infrastructure Architecture	>=99.95%	Per 0.5% breach of target penalty shall be Rs. 10,000. Maximum penalty of 5 % of quarterly payment amount. Penalty will be deducted from the quarterly payments.

Severity Level

Below severity definition provide scenarios for incidents severity.

Severity Level	Description
Severity 1	Environment is down or major malfunction resulting in an inoperative 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
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 workaround or no workaround exists. The environment is usable but severely limited.
Severity 3	Moderate loss of performance resulting in multiple users (includes public users) impacted in their normal functions.

Sr. No	Parameter	Description	Threshold
1	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
2	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 60 minutes of problem reporting
3	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 & 95% of Severity 3 within 16 hours of problem reporting

15 Payment Terms

S. No.	Milestone	Payment
A	Successful Completion of activities as part of One Time Costs: 2. Setting up cloud infrastructure for all the scope applications for pre-production and production environment 3. Migration Services for existing applications	As per CSP's quote in the financial proposal Form 1.4 for One Time Costs
B	Operation and Maintenance Support Phase	Shall be paid quarterly on the basis of Pay as per Use model as per unit prices as specified in the Financial Proposal Form 1.5

Note: -

1. *All payments shall be upon completion and sign-off received from the Client for the respective milestones. Operations and Maintenance Support Phase Quarterly Payments shall be done after successful completion of services for the respective quarter.*
2. *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.*
3. *MITL will release the payment within 45 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. MITL shall be entitled to delay or withhold the payment of a disputed invoice or part of it delivered by CSP.*
4. *All recurring cloud and managed-services charges shall be billed quarterly in arrears, i.e. at the end of each completed quarter of service, on a pay-as-per-use basis at the unit rates quoted in the Commercial Bid.*
5. *Annual Maintenance Charges (AMC) for perpetually-licensed components during the Extension Period: The perpetual-licence components (including the APM and DAM solutions) shall include all OEM support, updates and maintenance at no additional cost during the initial contract period. In the event the contract is extended under the Extension of Contract clause, AMC for these components shall be mutually agreed in writing prior to commencement of the extension, shall not exceed the prevailing market rates for equivalent support at that time, and shall be billed quarterly in arrears.*
6. *In case Go-Live is delayed, the corresponding operations and maintenance phase will start after the Go-Live has been completed.*
7. *All payments shall be made corresponding to the goods or services actually delivered, installed, or operationally accepted, as per the Contract Implementation Schedule, at unit prices and in the currencies specified in the Commercial Bids.*

16 Cloud Infrastructure Requirement

16.1 Bill of Quantity

Section	Line Items	Qty
VM Packs	VM PACK 1 : | 2 vcores, 2 GB RAM, 500 GB Performance Storage	2
	VM PACK 2 : | 2 vcores, 4 GB RAM, 500 GB Performance Storage	3
	VM PACK 3 : | 2 vcores, 8 GB RAM, 500 GB Performance Storage	8
	VM PACK 4 : | 4 vcores, 6 GB RAM, 500 GB Performance Storage	2
	VM PACK 5 : | 4 vcores, 8 GB RAM, 500 GB Performance Storage	11
	VM PACK 6 : | 4 vcores, 16 GB RAM, 500 GB Performance Storage	2
	VM PACK 7 : | 4 vcores, 32 GB RAM, 500 GB Performance Storage	4
	VM PACK 8 : | 4 vcores, 64 GB RAM, 500 GB Performance Storage	5
	VM PACK 9 : | 8 vcores, 8 GB RAM, 500 GB Performance Storage	2
	VM PACK 10 : | 8 vcores, 12 GB RAM, 500 GB Performance Storage	4
	VM PACK 11 : | 8 vcores, 16 GB RAM, 500 GB Performance Storage	5
	VM PACK 12 : | 8 vcores, 32 GB RAM, 500 GB Performance Storage	7
	VM PACK 13 : | 8 vcores, 52 GB RAM, 500 GB Performance Storage	2
	VM PACK 14 : | 8 vcores, 64 GB RAM, 500 GB Performance Storage	1
	VM PACK 15 : | 12 vcores, 6 GB RAM, 500 GB Performance Storage	4
	VM PACK 16 : | 12 vcores, 52 GB RAM, 500 GB Performance Storage	2
	VM PACK 17 : | 12 vcores, 64 GB RAM, 500 GB Performance Storage	1
	VM PACK 18 : | 16 vcores, 8 GB RAM, 500 GB Performance Storage	1
	VM PACK 19 : | 16 vcores, 32 GB RAM, 500 GB Performance Storage	1
	VM PACK 20 : | 16 vcores, 64 GB RAM, 500 GB Performance Storage	4
	VM PACK 21 : | 32 vcores, 64 GB RAM, 500 GB Performance Storage	1
Storage	High Performance Storage	50 TB
	Backup Storage	40 TB
	Object Storage	20 TB
Software Licenses	CentOS	19 No.
	Windows OS	75 No.
	Alma Linux	10 No.

	Ubuntu	11 No.
	RHEL - Small Instance	3 No.
	RHEL - Large Instance	5 No.
	Backup Agent	72 No.
	MSSQL Standard Edition	6 No.
	MSSQL Express Edition	4 No.
	SUSE for SAP Application	4 No.
	PostgreSQL Community	2 No.
	Mongo DB Community Edition	1 No.
	MySQL DB - Enterprise Edition	4 No.
	Email as a service – per ID	80 No.
Network Connectivity & Security	Antivirus + HIPS	72 No.
	Load Balancer as a Service	2 No.
	UTM Firewall with 1 Gbps throughput	2 No.
	Web Application firewall	2 No.
	Internet Bandwidth - Speed Based	100 Mbps
	Public IPs	21 No.
	SIEM	72 No.
	DDOS Mitigation as a Service	1 No.
	Domain SSL Certificate Wildcard	1 No.
	Application Performance Monitoring – Perpetual License	50 No.
	Database Activity Monitoring – Perpetual License	15 No.
	Vulnerability Scanning - Monthly twice	2 No.
	VAPT (Yearly twice)	1 No.
	Access control as a service	72 No.
Managed Services	Operating System Management Services per VM	72 No.
	Database Managed Service per VM	70 No.
	Backup Management per VM	45 No.
	Storage Management Services per VM	80 No.
	UTM Firewall Management Services	2 No.

	Load Balancer Management Services	2 No.
	Cloud Monitoring - Software	72 No.

- *All security components CSP has to factor as per the MeitY guidelines & relevant Indian IT acts.*
- *The quantities indicated in the Bill of Materials are indicative/estimated and are provided for the purpose of bid evaluation and price comparison only. The actual quantities provisioned may vary at the time of deployment and during the contract period based on the Department's actual requirements. Billing shall be on a pay-as-per-use basis at the unit rates quoted in the Commercial Bid, and the Department shall pay only for resources actually provisioned and consumed. Any addition or reduction of resources shall be charged/adjusted at the same quoted unit rates (and, for items not in the BOM, at the rates discovered through the optional rate card).*
- *All the services related to OS, DB, Networking and Security must be part of the solution proposed by CSP.*
- *Any item / material either hardware or software required to meet the functionality specified in the RFP document whose related component is missing in the above table has to be accounted by the Bidder and the cost of the same is assumed to be reflected and taken care in the cost specified to the Client by the Bidder in the financial bid. The Client is liable only to pay the Contract costs as per the payment terms mentioned to the Bidder to meet all the requirements as specified in the bidding documents and as per actual consumption of the items listed in the Recurring Costs Table given above plus as per the RFP terms and conditions.*
- *The Contract Cost shall be inclusive of all the installation, commissioning, testing and any other costs that might be incurred by the Bidder during the duration of the contract.*
- *Client shall be paying for cloud and managed services quarterly based on Client's actual usage on the basis of pay as per use model.*
- *Unit Rates provided as part of the Recurring Costs Table above shall be valid for entire duration of the Contract.*
- *Bidder can modify the servers compute, RAM and cores provided in the table above with only same or higher configuration.*
- *Unit price shall be provided for the line items being proposed, wherever applicable.*
- *Additional software solutions required for running MITL operations on cloud infrastructure shall be proposed and cost provided for the same in pay as per use model.*
- *MITL has the right to increase/ decrease the quantities and the IT infrastructure and the Total cost will be adjusted as per the unit costs indicated above on the basis of a pay-as-use model. There shall be no restriction on the increase or decrease of the quantities. The unit rates provided in the table above shall be used as a basis for any quantity increase during the course of the Contract.*
- *MITL shall have liberty to order additional cloud service items, at the rates offered in the financial proposal and also from market place at agreed terms and conditions.*
- *Requirements presented in Recurring Cost table provided above will be optimized for Project conditions at time of award and during detailed design phase of the Project.*

CSP technical and functional compliance for Key components and operations

1. Web Application Firewall

#	Description	Compliance (Y/N)
1	Cloud platform should provide Web Application Filter for OWASP (Open Web Application Security Project) Top 10 protection	
2	Service provider WAF should be able to support multiple website security.	
3	Service provider WAF should be able to perform packet inspection on every request covering all 7 layers.	
4	Service provider WAF should be able to block invalidated requests.	
5	Service provider WAF should be able to block attacks before it is posted to website.	
6	Service provider WAF should have manual control over IP/Subnet. i.e., Allow or Deny IP/Subnet from accessing website.	
7	The attackers should receive custom response once they are blocked.	
8	Service provider must offer provision to customize response of vulnerable requests.	
9	Service provider WAF should be able to monitor attack incidents and simultaneously control the attacker IP.	
10	Service provider WAF should be able to Whitelist or Backlist IP/Subnet.	
11	Service provider WAF should be able to set a limit to maximum number of simultaneous requests to the web server & should drop requests if the number of requests exceed the threshold limit.	
12	The WAF should be able to set a limit to maximum number of simultaneous connections per IP. And should ban / block the IP if the threshold is violated.	
13	WAF should be able to set a limit to maximum file size, combined file size in bytes	
14	WAF should be able to limit allowed HTTP versions, request content type, restricted extensions & headers	
15	Service provider WAF should be able to limit maximum number of arguments, argument name, value, value total length etc.	

#	Description	Compliance (Y/N)
16	Should be able to BAN an IP for a customizable specified amount of time if the HTTP request is too large.	
17	Should be able to limit maximum size of request body entity in bytes	
18	The WAF should be able to close all the sessions of an IP if it is ban.	
19	Should be able to Ban IP on every sort of attack detected and the time span for ban should be customizable. There should be a custom response for Ban IP.	
20	The WAF access and security Dashboard should show a graphical representation of	
	A) For access report analysis purpose the Dashboard should contain following information:	
	i) Number of hits by status code	
	ii) HTTP status code wise hits	
	iii) HTTP methods wise hits	
	iv) Client browser wise hits	
	v) Client Operating system wise hits	
	vi) Traffic(No. of hits) per URL	
	vii) Average bytes received per request	
	viii) Average bytes sent per request	
	ix) Average time elapsed per request	
	B) For security report analysis purpose the Dashboard should contain following information:	
	i) Average score by status code	
	ii) Distribution of blocked requests	
	iii) Number of blocked requests	
	iv) OWASP Top 10 requests	
	v) Reputation tags	
	vi) IP list reputation	

#	Description	Compliance (Y/N)
	C) For network incoming and outgoing traffic captured by WAF packet filter dashboard should contain following information:	
	i) Number of packet hits	
	ii) Source IP, Destination IP wise hits	
	iii) Firewall actions(allow, deny) wise hits	
	iv) Requests per destination port wise hits	
	D) Geo map of number of hits by country	
21	WAF should support different policies for different web applications.	
22	Vendor to ensure 24x7x365 availability of WAF service.	
23	WAF should support different policies for different application section (different security zones within the app).	
24	WAF should support IP Reputation DB (DB including blacklisted IP Address, IP Address, Anonymous Proxy, Botnets, Windows Exploit etc.) along with Client Source IP address based Security Policy and dynamic source IP blocking.	
25	WAF should enforce file upload control based on file type, size etc.	
26	WAF should detect known malicious users who are often responsible for automated and botnet attacks. Malicious users may include malicious IP addresses or anonymous proxy addresses.	
27	WAF should support detection only, blocking and transparent mode.	
28	WAF solution should be capable of handling IPV4 and IPV6 traffic.	
29	WAF solution should ensure compliance and advanced protection against industry standards such as OWASP Top 10 vulnerabilities etc.	
30	Vendor must monitor, manage & maintain the WAF solution on a 24x7 basis.	
31	WAF should provide a real-time dashboard with data such as top attacks view, traffic monitoring view, etc.	
32	WAF should provide role based access control for the dashboard (role based multiple login accounts both primary and secondary to be provided).	

#	Description	Compliance (Y/N)
33	WAF should provide detailed reports for all web application attacks.	
34	WAF should be able to decrypt the SSL traffic to analyse the HTTP data and should be able to re-encrypt the SSL traffic.	
35	WAF should support SSL offloading.	
36	WAF should support body inspection, content injection, backend compression, validation of UTF8 Encoding, XML Inspection.	
37	WAF should block invalid BODY.	
38	WAF should log all transactions for auditing purpose.	
39	WAF should block desktop users User-Agent, crawlers User-Agent, suspicious User-Agent.	
40	WAF should have customizable scoring policy for each request and can block request if global score exceeds.	
41	WAF should have DOS and BF protection for all or specific URLs.	
42	WAF should have learning mode to create whitelist/blacklist rules and also block attack in learning mode.	
43	WAF should verify SSL certificate, certificate name, expiration and cipher suites. Also control over accepted TLS/SSL protocol, cipher order, CRL verification, HTTP public key pinning, OCSP stapling.	
44	WAF should allow to inject Request and Response headers for applications.	
45	WAF should support Content and URL rewriting policies.	
46	WAF should send proxy HTTP headers to backend, r rewrite cookie path, backend' s cookies encryption and override backend server HTTP errors.	
47	WAF should support force HTTP to HTTPS redirection.	
48	WAF should support URL specific rulesets and should allow/deny specific countries(GeoIP) for applications.	
49	WAF should have OS level firewall to PASS/BLOCK traffic inbound/outbound traffic	
50	WAF should allow to create custom rules for application.	
51	WAF should support Active-Active/Active-Passive failover.	

2. SIEM Service

Sr. No.	SIEM Description	Compliance (Y/N)
1	The solution should be able to handle a minimum of Avg 5.06 Eps / Device	
2	The solution should be scalable by adding additional receivers and still be managed through a single, unified security control panel.	
3	The solution should be capable of real time analysis and reporting.	
4	The platform should not require a separate RDBMS for log collection, web server or any kind of application software for its installation.	
5	The solution should be able to assign risk scores to your most valuable asset. The risk value could be assigned to a service, application, specific servers, a user or a group. The solution should be able to assign and consider the asset criticality score before assigning the risk score.	
6	The relative risk of each activity should be calculated based on values assigned by the Asset Administrator.	
7	The activities should be separated by levels of risk for the company: very high, high, medium, low and very low.	
8	The SIEM receiver/log collection appliance must be an appliance based solution and not a software based solution to store the data locally, if communication with centralized correlator is unavailable.	
9	The solution should be able to collect logs via the following ways as inbuilt into the solution: Syslog, OPSec, agent-less WMI, RDEP, SDEE, FTP, SCP, External Agents such as Adiscon.	
10	The solution should provide a data aggregation technique to summarize and reduce the number of events stored in the master database.	
11	The solution should provide a data store which is compressed via flexible aggregation logic.	
12	The data collected from the receiver should be forwarded in an encrypted manner to SIEM log storage.	
13	The solution should provide pre-defined report templates. The reports should also provide reports out of the box such as ISO 27002.	

Sr. No.	SIEM Description	Compliance (Y/N)
14	The solution should provide reports that should be customizable to meet the regulatory, legal, audit, standards and management requirements.	
15	The solution should also provide Audit and Operations based report, Native support for Incident management workflow.	
16	The solution should have single integrated facility for log investigation, incident management etc. with a search facility to search the collected raw log data for specific events or data.	
17	A well-defined architecture along with pre and post installation document need to be shared by the bidder.	
18	The solution should have a scalable architecture, catering multi-tier support and distributed deployment.	
19	The solution should support collection of events/logs and network flows from distributed environment(s).	
20	The solution should correlate security/network events to enable the SOC to quickly prioritize it's response to help ensure effective incident handling.	
21	The solution should integrate asset information in SIEM such as categorization, criticality and business profiling and use the same attributes for correlation and incident management.	
22	The solution should provide remediation guidance for identified security incident:	
23	a) Solution should be able to specify the response procedure (by choosing from the SOPs) to be used in incident analysis/remediation.	
24	The solution should facilitate best practices configuration to be effectively managed in a multi-vendor and heterogeneous information systems environment.	
25	The solution should provide capability to discover similar patterns of access, communication etc. occurring from time to time, for example, slow and low attack.	
26	The solution should perform regular (at least twice a year) health check and fine tuning of SIEM solution and should submit a report.	
27	The solution should share the list of out of the box supported devices/log types.	

Sr. No.	SIEM Description	Compliance (Y/N)
28	The solution should support hierarchical structures for distributed environments. The solution should have capability for correlation of events generated from multiple SIEM(s) at different location in single management console.	
29	The event correlation on SIEM should be in real time and any delay in the receiving of the events by SIEM is not acceptable.	
30	The solution should support internal communication across SIEM-components via well-defined secured channel. UDP or similar ports should not be used.	
31	Event dropping/caching by SIEM solution is not acceptable and same should be reported and corrected immediately.	
32	The solution should be able to facilitate customized dashboard creation, supporting dynamic display of events graphically.	
33	The solution should be able to capture all the fields of the information in the raw logs.	
34	The solution should support storage of raw logs for forensic analysis.	
35	The solution should be able to integrate logs from new devices into existing collectors without affecting the existing SIEM processes.	
36	The solution should have capability of displaying of filtered events based on event priority, event start time, end time, attacker address, target address etc.	
37	The solution should support configurable data retention policy based on organization requirement.	
38	The solution should provide tiered storage strategy comprising of online data, online archival, offline archival and restoration of data. Please elaborate on log management methodology proposed.	
39	The solution should compress the logs by at least 70% or more at the time of archiving.	
40	The solution should have capability for log purging and retrieval of logs from offline storage.	
41	Solution should be capable of replicating logs in Synchronous as well as Asynchronous mode for replication from Primary site to DR site.	

Sr. No.	SIEM Description	Compliance (Y/N)
42	The solution should provide proactive alerting on log collection failures so that any potential loss of events and audit data can be minimized or mitigated.	
43	The solution should provide a mechanism (in both graphic and table format) to show which devices and applications are being monitored and determine if a continuous set of collected logs exist for those devices and applications.	
44	The solution should support automated scheduled archiving functionality into file system.	
45	The solution should support normalization of real time events.	
46	The solution should provide a facility for logging events with category information to enable device independent analysis.	
47	The platform should be supplied on Hardened OS embedded in Hardware / Virtual Appliance. The storage configuration should offer a RAID configuration to allow for protection from disk failure.	
48	The platform should have High Availability Configuration of necessary SIEM components to ensure there is no single point of failure. Please describe the architecture proposed to meet this requirement.	
49	By default at the time of storage, solution should not filter any events. However, solution should have the capability of filtering events during the course of correlation and report generation.	
50	The solution should ensure the integrity of logs. Compliance to regulations should be there with tamper-proof log archival.	
51	The solution should be able to continue to collect logs during backup, de-fragmentation and other management scenarios.	
52	The solution should support collection of logs from all the devices quoted in RFP.	
53	The collection devices should support collection of logs via the following but not limited methods:	
54	1. Syslog over UDP / TCP	
55	2. SNMP	
56	3. ODBC (to pull events from a remote database)	
57	4. FTP (to pull a flat file of events from a remote device that	

Sr. No.	SIEM Description	Compliance (Y/N)
	can't directly write to the network)	
58	5. Windows Event Logging Protocol	
59	7. NetBIOS	
60	The solution should allow a wizard / GUI based interface for rules (including correlation rules) creation as per the customized requirements. The rules should support logical operators for specifying various conditions in rules.	
61	The solution should support all standard IT infrastructure including Networking & Security systems, OS, RDBMS, Middleware, Web servers, Enterprise Management System, LDAP, Internet Gateway, Antivirus, and Enterprise Messaging System, Data loss prevention (DLP) etc.	
62	The solution should have provision for integration of the following:	
63	d) Inclusion of "Application context".	
64	Solution should have license for minimum 10 users for SIEM administration.	
65	The solution should have the ability to define various roles for SIEM administration, including but not limited to: Operator, Analyst, SOC Manager etc. for all SIEM components.	
66	The solution should support SIEM management process using a web based solution.	
67	The solution should support the following co- relation:	
68	Statistical Threat Analysis - To detect anomalies.	
69	Susceptibility Correlation - Raises visibility of threats against susceptible hosts.	
70	Vulnerability Correlation - Mapping of specific detected threats to specific / known vulnerabilities	
71	Rules based Correlation - The solution should allow creating rules that can take multiple scenarios like and create alert based on scenarios.	
72	Solution should have capability to correlate based on the threat intelligence for malicious domains, proxy networks, known bad IP's and hosts.	

Sr. No.	SIEM Description	Compliance (Y/N)
73	The solution should provide ready to use rules for alerting on threats e.g., failed login attempts, account changes and expirations, port scans, suspicious file names, default usernames and passwords, High bandwidth usage by IP, privilege escalations, configuration changes, traffic to non-standard ports, URL blocked, accounts deleted and disabled, intrusions detected etc.	
74	The solution should support the following types of correlation conditions on log data:	
75	a) One event followed by another event	
76	b) Grouping, aggregating, sorting, filtering, and merging of events.	
77	c) Average, count, minimum, maximum threshold etc.	
78	Solution should provide threat scoring based on:	
79	a) Host, network, priority for both source	
80	& destination	
81	b) Real-time threat, event frequency, attack level etc.	
82	The solution should correlate and provide statistical anomaly detection with visual drill down data mining capabilities.	
83	The solution should have the capability to send notification messages and alerts through email, SMS, etc.	
84	The solution should support RADIUS and LDAP / Active Directory for Authentication.	
85	The solution should provide highest level of enterprise support directly from OEM.	
86	The solution should provide a single point of contact directly from OEM for all support reported OEM.	
87	The solution should ensure continuous training and best practice updates for onsite team from its backend resources.	
88	Solution should support log integration for IPv4 as well as for IPv6.	
89	Solution should provide inbuilt dashboard for monitoring the health status of all the SIEM components, data insert/retrieval time, resource utilization details etc.	

Sr. No.	SIEM Description	Compliance (Y/N)
90	Solution should support at least 100 default correlation rules for detection of network threats and attacks. The performance of the solution should not be affected with all rules enabled.	
91	The central management console/ Enterprise Security managers/receivers should be in high availability.	
92	24/7 extensive monitoring of the cloud services and prompt responses to attacks and security incidents	
93	Recording and analysing data sources (e.g. system status, failed authentication attempts, etc.)	
94	24/7 contactable security incident handling and troubleshooting team with the authority to act	
95	Obligations to notify the customer about security incidents or provide information about security incidents potentially affecting the customer	
96	Provision of relevant log data in a suitable form	
97	Logging and monitoring of administrator activities	

17 Qualification Documents and Technical Proposal - Standard Forms

Table of Contents

17.1 Form T1- Qualification Documents and Proposal Submission Form

[On the Letter head of the Bidder]

{Location, Date}

To:

Managing Director,

Maharashtra Industrial Township Limited,
Udoyg Sarathi, MIDC Office, Marol Industrial Area, Andheri (East),
Mumbai, Maharashtra, India – 400 093

Ref: RFP for Selection of Service Provider (Cloud Hosting and Managed Service) to Setup, Migrate, and Manage Data Centre (DC) and Disaster Recovery (DR) site for MITL on Cloud

Dear Sir:

We, the undersigned, offer to provide the Solution, and Service Provider (Cloud Hosting and Managed Service) to Setup, Migrate, and Manage Data Centre (DC) and Disaster Recovery (DR) site for MITL on Cloud in accordance with your Request for Qualification cum Request for Proposal dated [Insert Date]. We are hereby submitting our Proposal, which includes the Qualification Documents and our Financial Proposal, each in a separate sealed envelope.

If negotiations are held during the period of validity of the Proposal, we undertake to negotiate in accordance with the RFP. Our proposal is binding upon us, subject only to the modifications resulting from negotiations in accordance with the RFP.

We hereby declare that:

(a) The Client will be relying on the information provided in the Proposal and the documents accompanying the Proposal for the selection of the CSP. All the information and statements made in this Proposal are true, nothing has been omitted which renders such information misleading and we accept that any misinterpretation or misrepresentation contained in this Proposal may lead to our disqualification by the Client.

(b) All documents accompanying our Proposal are true copies of their respective originals. We will make available to the Client any additional information it may find necessary or require to authenticate or evaluate the Proposal.

(c) We and our Affiliates are not submitting more than one or separate Proposals.

(d) We or any of our Affiliates have not been charge-sheeted by any agency of the government or convicted by a court of law, indicted or have had adverse orders passed by a regulatory authority which could cast a doubt on our ability to execute the Contract.

(e) No investigation by a regulatory authority is pending either against us or any of our Affiliates or against our chief executive officer or any of our directors/managers/employees.

(f) If due to any change in facts or circumstances during the bid process, we attract the provisions of disqualification in terms of the provisions of this RFP, we shall inform the Client of the same immediately.

(g) We meet the Qualification Criteria and all other requirements of the RFP and are qualified to submit a Proposal, We have not directly or indirectly through an agent engaged or indulged in any corrupt practice, fraudulent practice, coercive practice, collusive practice, undesirable practice or restrictive. We undertake to continue to abide by and ensure that our Personnel comply with the Client's policy with regard to corrupt and fraudulent practices.

(h) We or our Affiliates, suppliers, or service providers for any part of the Contract, are not subject to any temporary suspension and have not been barred by any government or government instrumentality in India or in any other jurisdiction to which we or our Affiliates belong or in which we or our Affiliates conduct business or by any multilateral funding agency, from participating in any project or being awarded any contract or being given any funding and no such suspension or bar subsists on the Proposal Due Date.

(i) In the last 5 (five) years, we or our Affiliates have neither been expelled from any project or contract by any government or government instrumentality nor have had any contract terminated by any government or government instrumentality for breach on our part.

(j) If we are selected as the CSP, we undertake the Contract as prescribed in the RFP and agree not to seek any changes in the aforesaid form and agree to abide by the same. We will provide the Goods and Services on the basis of the proposed Solution.

(k) Our Proposal is binding upon us and is subject to any modifications resulting from the Contract negotiations.

(l) We have carefully analysed the RFP and all related information. We understand that except to the extent as expressly set forth in the Contract, we shall have no claim, right or title arising out of any documents or information provided to us by the Client or in respect of any matter arising out of or concerning or relating to the bid process including the award of the Contract.

(m) Our Financial Proposal has been quoted by us after taking into consideration all the terms and conditions stated in the RFP, the Technical Requirements, the draft Contract, our own estimates of costs and after a careful assessment of all the conditions that may affect the Work.

(n) We irrevocably waive any right or remedy which we may have at any stage at law or howsoever arising to challenge the criteria for evaluation or question any decision taken by the Client in connection with the evaluation of the Proposals, selection of the Bidder, or in respect of this Project and the terms and implementation thereof.

(o) We acknowledge the right of the Client to reject our Proposal without assigning any reason and we hereby waive, to the fullest extent permitted by applicable law, our right to challenge the same on any account whatsoever.

(p) We acknowledge the right of the Client to cancel the bid process and not award the Contract, without assigning any reason and without incurring any liability to the Bidders and we hereby waive, to the fullest extent permitted by applicable law, our right to challenge the same on any account whatsoever.

(q) We undertake, if our Proposal is accepted and the Contract is signed, to initiate the Services no later than the date indicated in the RFP document

(r) We shall make available to the Client any additional information it may deem necessary or require for supplementing or authenticating the Proposal.

(s) We acknowledge the right of Client to reject our application without assigning any reason or otherwise and hereby waive our right to challenge the same on any account whatsoever.

(t) We further certify that no investigation by a regulatory authority is pending either against us or against our affiliates or against our CEO or any of our Directors/ Managers/ employees.

We remain,

Yours sincerely,

Authorized Signature {In full and initials}: _____

Name and Title of Signatory: _____

Address: _____

Contact information (phone and e-mail): _____

17.2 FORM T2- Details of The Bidder

(To be submitted on the letterhead of the Bidder)

All individual firms that are bidding must complete the information in this form.

1. (a) Name:

   (b) Country of incorporation:

   (c) Date of incorporation and/or commencement of business:

2. Brief description of the company including details of its main lines of business and proposed role and responsibilities in this assignment [*Note: Such description shall not exceed 5 type-written pages.*]:

3. Details of individual who will serve as the point of contact/ communication for the Client[2]:

   (a) Name:

   (b) Designation:

   (c) Company:

   (d) Address:

   (e) Telephone Number:

   (f) E-Mail Address:

   (g) Fax Number:

4. Particulars of the Authorised Signatory of the Bidder:

   (a) Name:

   (b) Designation:

   (c) Address:

   (d) Telephone Number:

   (e) E-Mail Address:

   (f) Fax Number:

17.3 FORM T3- Format for Power of Attorney for Authorised Representative

(To be executed as per Applicable Laws)

Know all men by these presents, We, [name of organization and address of the registered office] do hereby constitute, nominate, appoint and authorise Mr / Ms [name], son/ daughter/ wife of [name], and presently residing at [address], who is presently employed with/ retained by us and holding the position of [designation] as our true and lawful attorney (hereinafter referred to as the "Authorised Representative"), to do in our name and on our behalf, all such acts, deeds and things as are necessary or required in connection with or incidental to submission of our Proposal for selection as Cloud Service Provider for [name of assignment], to be developed by the Client including but not limited to signing and submission of all applications, proposals and other documents and writings, participating in pre-bid and other conferences and providing information/responses to the Client, representing us in all matters before the Client, signing and execution of all contracts and undertakings consequent to acceptance of our proposal and generally dealing with the Client in all matters in connection with or relating to or arising out of our Proposal for the said Project and/or upon award thereof to us until the entering into of the Contract with the Client.

AND, we do hereby agree to ratify and confirm all acts, deeds and things lawfully done or caused to be done by our said Authorised Representative pursuant to and in exercise of the powers conferred by this Power of Attorney and that all acts, deeds and things done by our said Authorised Representative in exercise of the powers hereby conferred shall and shall always be deemed to have been done by us.

The Power of Attorney will continue to be valid so long as the said Authorized Representative is in the employment of the Company.

IN WITNESS WHEREOF WE, [name of organization], THE ABOVE NAMED PRINCIPAL HAVE EXECUTED THIS POWER OF ATTORNEY ON THIS [date in words] DAY OF [month] [year in 'yyyy' format].

For [name and registered address of organization]

[Signature]

[Name]

[Designation]

Witnesses:

1 [Signature, name and address of witness]

2 [Signature, name and address of witness]

Accepted

[Signature]

[Name][Designation]

[Address]

Notes:

a. *The mode of execution of the Power of Attorney should be in accordance with the procedure, if any, laid down by the applicable law and the charter documents of the executant(s) and when it is so required the same should be under seal affixed in accordance with the required procedure.*

b. *Wherever required, the Bidder should submit for verification the extract of the charter documents and other documents such as a resolution/power of attorney in favour of the person executing this Power of Attorney for the delegation of power hereunder on behalf of the Bidder.*

17.4 FORM T4- Financial Qualification of the Bidder

Certificate from the Statutory Auditor or Practicing CA Firm

CERTIFICATE

This is to certify that the annual turn over of _____[full name of company] [registered address] is as follows :

S. No.	Financial Years	Annual turnover
1	2022-2023	
2	2023-2024	
3	2024-2025	
Total Turnover (Rs)		
Average Turnover (Rs)		

(A) Networth as on 31st March, 2025, Rs._____

(B) Further it is certified that the company has not applied for Corporate Debt Restructuring (CDR) as on date of bid submission.

Signature of Authorized Signatory:

Name & Seal of the Auditor or Practicing CA Firm

(Bidders shall provide financial information to demonstrate that they meet the requirements stated in Qualification Criteria. Each Bidder shall complete this form. If necessary, separate sheets shall be used to provide complete banker information. A copy of the audited balance sheets shall be attached)

17.5 FORM T5- Technical Qualification – Qualifying Projects

[Use a separate sheet for each contract]

Name of Bidder:

1.	Number of contracts	
	Name of contract	
	Country	
2.	Name of Client	
3.	Client address with Contact Details	
4.	Nature of Services and special features relevant to the contract for which the Bidding Documents are issued:	
5.	Contract role (check one) □ Prime Bidder □ Management Contractor □ Sub-Contractor □ Partner in a Joint Venture	
6.	Amount of the total contract/subcontract/partner share (in specified currencies at completion, or at date of award for current contracts) Total contract: INR_____; Subcontract: INR_____; Partner share: INR_____;	
8.	Date of award: Date of Commissioning:	
9.	Contract was completed _____ months ahead/behind original schedule (if behind, provide explanation).	
10.	Contract was completed INR _____ equivalent under/over original contract amount (if over, provide explanation).	
11.	Special contractual/technical requirements:	

(Name and Signature of Authorized Signatory)

Note:

TR 1*For each Eligible Assignment, the Bidder should indicate the duration of the assignment, the contract amount, the amount paid to the Bidder and the Bidder's role/involvement.*

TR 2*Bidders are expected to provide information in respect of each Eligible Assignment in this Appendix. Each Eligible Assignment must comply with the requirements set out in the Qualification Criteria*

TR 3*Please limit the description of the project to four (04) single sided pages (two double sided pages) A4 size sheet of paper. Descriptions exceeding four A4 size sheet of paper shall not be considered for evaluation.*

17.6 Form T6- Format for Affidavit Certifying that Bidder are Not Blacklisted

(On a Stamp Paper of Rs. 100/- value and duly notarized)

Affidavit

I M/s. ……, (the name of the Bidder and addresses of the registered office) hereby certify and confirm that we are not barred or blacklisted by any Central / State Government Department or Central / State PSUs from participating in any project or being awarded any contract, either individually or as member of a consortium and no such bar or blacklisting subsists as on the Proposal Due Date.

We further confirm that we are aware our Proposal for the **RFP for Selection of Service Provider (Cloud Hosting and Managed Service) to Setup, Migrate, and Manage Data Centre (DC) and Disaster Recovery (DR) site for MITL on Cloud,** Project would be liable for rejection in case any material misrepresentation is made or discovered with regard to the requirements of this RFP at any stage of selection and/or thereafter during the term of the Contract.

Dated this ……..Day of ……., 20….

NAME OF THE BIDDER

…….

SIGNATURE OF THE AUTHORISED PERSON

…….

NAME OF THE AUTHORISED PERSON

17.7 FORM T7- Bid Compliance Undertaking

[The Bidder shall submit an undertaking (on company letterhead and should be signed and stamped) confirming compliance to all business, functional and technical requirements as specified in this Scope of work in the RFP.]

The Bidder shall submit undertaking with following points:

1. We hereby confirm that our proposal is fully and truly compliant as per the terms and conditions of this RFP without any deviations.

Proposals received without Bid Compliance Undertaking shall be rejected as non-responsive. Proposals with missing, incomplete, or ambiguous responses regarding compliance may be deemed non-responsive. Bidders must submit fully compliant proposal with all the requirements as defined in the document. Client reserves the right to request more information for any or all responses listed after the bid submission deadline during the evaluation process.

17.8 FORM T8- Form of EMD (DD)

Date:

In Favour of: M/s Maharashtra Industrial Township Limited (MITL), Payable at Mumbai

- Any e-Bid not secured in accordance with above shall be treated as non-responsive and rejected by the MITL.
- Unsuccessful Bidder's EMD will be returned as promptly as possible after the opening of the Price Bid.
- The successful Bidder's e-Bid EMD will be adjusted with Performance Security to be submitted by the Bidder upon signing the contract.
- The EMD may be forfeited:
- If Bidder (i) withdraws its e-Bid during the period of e-Bid validity specified by the Bidder on the e- bid form: or (ii) does not accept the correction of errors or (iii) modifies its e-Bid price during the period of e-Bid validity specified by the Bidder on the form.
- In case of a successful Bidder, if the Bidder fails to sign the contract with the MITL.

Financial Proposal (Price Schedule) - Standard Forms

Table of Contents

17.9 Financial Proposal Submission

General

1. The Price Schedules are divided into separate Schedules as follows:

1. Financial Proposal Submission Form;
2. Grand Summary Cost Table;
3. One Time Costs;
4. Recurring Costs.
5. DRC / Secondary DC Costs (Not to be evaluated)

2. The Schedules do not generally give a full description of the information technologies to be supplied, installed, and operationally accepted, or the Services to be performed under each item. However, it is assumed that Bidders shall have read the Terms of Reference and other sections of these RFP Documents to ascertain the full scope of the requirements associated with each item prior to filling in the rates and prices. The quoted rates and prices shall be deemed to cover the full scope of these Terms of Reference, as well as overhead and profit.
3. If Bidders are unclear or uncertain as to the scope of any item, they shall seek clarification in accordance with the Instructions to Bidders in the RFP Documents prior to submitting their bid.

Pricing

4. Prices shall be filled in indelible ink, and any alterations necessary due to errors, etc., shall be initialed by the Bidder. As specified in the Bid Data Sheet, prices shall be fixed and firm for the duration of the Contract.
5. Bid prices shall be quoted in the manner indicated and in the currencies specified in RFP. Prices must correspond to items of the scope and quality defined in the Technical Requirements or elsewhere in these RFP Documents.
6. The Bidder must exercise great care in preparing its calculations, since there is no opportunity to correct errors once the deadline for submission of bids has passed. A single error in specifying a unit price can therefore change a Bidder’s overall total bid price substantially, make the bid noncompetitive, or subject the Bidder to possible loss.
7. Payments will be made to the Bidder in the currency or currencies indicated under each respective item in INR only. The price of an item should be unique regardless of installation site.

17.10 Financial Proposal Submission Form

[Location], [Date]

To

Managing Director,

Maharashtra Industrial Township Limited,

Udyog Sarathi, MIDC Office, Marol Industrial Area, Andheri (East),

Mumbai, Maharashtra – 400093

India

Dear Sir,

Subject: RFP for Selection of Service Provider (Cloud Hosting and Managed Service) to Setup, Migrate, and Manage Data Centre (DC) and Disaster Recovery (DR) site for MITL on Cloud

We, the undersigned, offer to provide the Managed services for RFP for Selection of Service Provider (Cloud Hosting and Managed Service) to Setup, Migrate, and Manage Data Centre (DC) and Disaster Recovery (DR) site for MITL on Cloud, in accordance with your Request for Qualification – cum - Request for Proposal dated [date] and our Proposal. Our attached Financial Proposal is for the sum of **[amount(s) in words and figures].**

Our Financial Proposal shall be binding upon us subject to the modifications resulting from arithmetic correction, if any, up to expiration of the validity period of the Proposal, i.e. **[date].** We further understand that the Financial Proposal (Recurring Costs – Form 1.5) is indicative and prepared by you for evaluation purposes only and the actual payments shall be based on pay-as-per-use model based on the terms and conditions of the RFP.

We undertake that, in competing for (and, if the award is made to us, in executing) the above contract, we will strictly observe the laws against fraud and corruption in force in India namely “Prevention of Corruption Act 1988”.

We understand you are not bound to accept any Proposal you receive.

We remain,

Yours sincerely,

Authorized Signature [In full and initials]:

Name and Title of Signatory:

Name of Firm:

Address:

17.11 Grand Summary Cost Table

S. No.	Description	Price (INR) (Exclusive of Taxes and inclusive of duties)	Price (INR) (Applicable Taxes)	Total Cost (INR) (Inclusive of Taxes & Duties)
1.	One-time Costs			
2	Recurring Costs for period of 24 Months			
3	**Grand Total (to Bid Submission Form)** = One Time Costs + Recurring Costs)	The Evaluated Bid Price (C) =		

Name of Bidder:	
Authorized Signature of Bidder:	

17.11.1 One Time Costs

S. No.	Description	One-Time Costs (INR) (exclusive of Taxes and inclusive of Duties	All Applicable Taxes (INR)	Total Cost (INR) (Inclusive of Taxes & Duties)
	One-time cost of setting up cloud infrastructure for all the scope applications for the pre-production and production environments			
	Migration Services for existing applications			
	Any other one-time costs with description			
	GRAND TOTAL			

Name of Bidder:	
Authorized Signature of Bidder:	

Notes:

1. *Any item/ material either hardware or software required to meet the functionality specified in the tender document whose related component is missing in the above table has to be accounted by the Bidder and the cost of the same is assumed to be reflected and taken care in the cost specified to the Client by the Bidder in the financial bid. The Client is liable only to pay the Contract costs as per the payment terms mentioned to the Bidder to meet all the requirements as specified in the bidding documents.*
2. *The Contract Cost shall be inclusive of all the installation, commissioning, testing and any other costs that might be incurred by the Bidder during the duration of the contract.*

17.11.2 Monthly Recurring Costs (For Evaluation Purposes Only)

Section	Line Items	Qty	Unit Price	Monthly Price (A)	OTC cost (B)
VM Packs	VM PACK 1 : | 2 vcores, 2 GB RAM, 500 GB Performance Storage	2			
	VM PACK 2 : | 2 vcores, 4 GB RAM, 500 GB Performance Storage	3			
	VM PACK 3 : | 2 vcores, 8 GB RAM, 500 GB Performance Storage	8			
	VM PACK 4 : | 4 vcores, 6 GB RAM, 500 GB Performance Storage	2			
	VM PACK 5 : | 4 vcores, 8 GB RAM, 500 GB Performance Storage	11			
	VM PACK 6 : | 4 vcores, 16 GB RAM, 500 GB Performance Storage	2			
	VM PACK 7 : | 4 vcores, 32 GB RAM, 500 GB Performance Storage	4			
	VM PACK 8 : | 4 vcores, 64 GB RAM, 500 GB Performance Storage	5			
	VM PACK 9 : | 8 vcores, 8 GB RAM, 500 GB Performance Storage	2			
	VM PACK 10 : | 8 vcores, 12 GB RAM, 500 GB Performance Storage	4			
	VM PACK 11 : | 8 vcores, 16 GB RAM, 500 GB Performance Storage	5			
	VM PACK 12 : | 8 vcores, 32 GB RAM, 500 GB Performance Storage	7			
	VM PACK 13 : | 8 vcores, 52 GB RAM, 500 GB Performance Storage	2			
	VM PACK 14 : | 8 vcores, 64 GB RAM, 500 GB Performance Storage	1			
	VM PACK 15 : | 12 vcores, 6 GB RAM, 500 GB Performance Storage	4			
	VM PACK 16 : | 12 vcores, 52 GB RAM, 500 GB Performance Storage	2			

	VM PACK 17 : | 12 vcores, 64 GB RAM, 500 GB Performance Storage	1			
	VM PACK 18 : | 16 vcores, 8 GB RAM, 500 GB Performance Storage	1			
	VM PACK 19 : | 16 vcores, 32 GB RAM, 500 GB Performance Storage	1			
	VM PACK 20 : | 16 vcores, 64 GB RAM, 500 GB Performance Storage	4			
	VM PACK 21 : | 32 vcores, 64 GB RAM, 500 GB Performance Storage	1			
Storage	High Performance Storage	50 TB			
	Backup Storage	40 TB			
	Object Storage	20 TB			
Software Licenses	CentOS	19 No.			
	Windows OS	75 No.			
	Alma Linux	10 No.			
	Ubuntu	11 No.			
	RHEL - Small Instance	3 No.			
	RHEL - Large Instance	5 No.			
	Backup Agent	72 No.			
	MSSQL Standard Edition	6 No.			
	MSSQL Express Edition	4 No.			
	SUSE for SAP Application	4 No.			
	PostgreSQL Community	2 No.			
	Mongo DB Community Edition	1 No.			
	MySQL DB - Enterprise Edition	4 No.			
	Email as a service – per ID	80 No.			
Network Connectivity & Security	Antivirus + HIPS	72 No.			
	Load Balancer as a Service	2 No.			
	UTM Firewall with 1 Gbps throughput	2 No.			
	Web Application Firewall	2 No.			
	Internet Bandwidth - Speed Based	100 Mbps			

	Public Ips	21 No.			
	SIEM	72 No.			
	DDOS Mitigation as a Service	1 No.			
	Domain SSL Certificate Wildcard	1 No.			
	Application Performance Monitoring – Perpetual License	50 No.			
	Database Activity Monitoring – Perpetual License	15 No.			
	Vulnerability Scanning - Monthly twice	2 No.			
	VAPT (Yearly twice)	1 No.			
	Access control as a service	72 No.			
Managed Services	Operating System Management Services per VM	72 No.			
	Database Managed Service per VM	70 No.			
	Backup Management per VM	45 No.			
	Storage Management Services per VM	80 No.			
	UTM Firewall Management Services	2 No.			
	Load Balancer Management Services	2 No.			
	Cloud Monitoring - Software	72 No.			
Grand Total for Recurring Costs (INR)- exclusive of Taxes					

Grand Total for Recurring Costs (Monthly Recuring +OTC) (INR) exclusive of Taxes	
Grand Total for Recurring Costs (Monthly Recuring +OTC) (INR) Including of Taxes	

Name of Bidder:	
Authorized Signature of Bidder:	

- *All security components CSP has to factor as per the MeitY guidelines & relevant Indian IT acts.*
- *The quantities indicated in the Bill of Materials are indicative/estimated and are provided for the purpose of bid evaluation and price comparison only. The actual quantities provisioned may vary at the time of deployment and during the contract period based on the Department's actual requirements. Billing shall be on a pay-as-per-use basis at the unit rates quoted in the Commercial Bid, and the Department shall pay only for resources actually provisioned and*

consumed. Any addition or reduction of resources shall be charged/adjusted at the same quoted unit rates (and, for items not in the BOM, at the rates discovered through the optional rate card).

- *All the services related to OS, DB, Networking and Security must be part of the solution proposed by CSP.*
- *Any item / material either hardware or software required to meet the functionality specified in the RFP document whose related component is missing in the above table has to be accounted by the Bidder and the cost of the same is assumed to be reflected and taken care in the cost specified to the Client by the Bidder in the financial bid. The Client is liable only to pay the Contract costs as per the payment terms mentioned to the Bidder to meet all the requirements as specified in the bidding documents and as per actual consumption of the items listed in the Recurring Costs Table given above plus as per the RFP terms and conditions.*
- *The Contract Cost shall be inclusive of all the installation, commissioning, testing and any other costs that might be incurred by the Bidder during the duration of the contract.*
- *Client shall be paying for cloud and managed services quarterly based on Client's actual usage on the basis of pay as per use model.*
- *Unit Rates provided as part of the Recurring Costs Table above shall be valid for entire duration of the Contract.*
- *Bidder can modify the servers compute, RAM and cores provided in the table above with only same or higher configuration.*
- *Unit price shall be provided for the line items being proposed, wherever applicable.*
- *Additional software solutions required for running MITL operations on cloud infrastructure shall be proposed and cost provided for the same in pay as per use model.*
- *MITL has the right to increase/ decrease the quantities and the IT infrastructure and the Total cost will be adjusted as per the unit costs indicated above on the basis of a pay-as-use model. There shall be no restriction on the increase or decrease of the quantities. The unit rates provided in the table above shall be used as a basis for any quantity increase during the course of the Contract.*
- *MITL shall have liberty to order additional cloud service items, at the rates offered in the financial proposal and also from market place at agreed terms and conditions.*
- *Requirements presented in Recurring Cost table provided above will be optimized for Project conditions at time of award and during detailed design phase of the Project.*

17.12 Monthly Cost for Disaster Recovery Centre (DRC) / Secondary Data Centre (DC) Costs (Not to be Evaluated)

The following rate card is for the purpose of discovering firm unit rates for additional/future line items that the Department may require during the contract period. The tentative quantity of one (1) against each item is indicative only and does not constitute any committed procurement by the Department.

The rates quoted in this rate card shall not form part of the evaluated commercial bid for QCBS evaluation; the commercial score shall be computed solely on the GRAND TOTAL of the Bill of Material above. The Department reserves the right to procure any quantity of these items, at the quoted unit rates, on an as-required basis during the contract period and any extension thereof.

All rate-card unit rates shall remain firm and shall be treated as ceiling rates for the duration of the initial contract period. For any item that also appears in the Bill of Material, the unit rate quoted in this rate card shall not exceed the equivalent unit rate derived from the Bill of Material. Any item left blank or quoted as zero/nil shall be treated as included at no extra cost. In the event the contract is extended under the Extension of Contract clause, the rate-card unit rates applicable during the extension period shall be mutually agreed in writing between the Department and the CSP prior to commencement of the extension, in the same manner as the other prices under the contract.

Sr. No	Item Title	Item Description	Tentative Quantity *	Unit of Measure	Unit Price (Inclusive of all taxes)
1	vCPU (1:1)	Per Virtual Core	1	No	
2	vCPU (1:2)	Per Virtual Core	1	No	
3	vRAM	Per GB Virtual RAM	1	No	
4	Block Storage	All SSD (1000 IOPs/TB)	1	TB	
5	Performance Storage	All SSD (3000 IOPs/TB)	1	TB	
6	Performance Storage	All SSD (5000 IOPs/TB)	1	TB	
7	Archive Storage	SAS/NL SAS	1	TB	
8	Backup Storage	SAS/NL SAS	1	TB	
9	Windows OS (2 vCores/License)	Latest	1	No	
10	Public IP	IPv4/IPv6	1	No	

11	Host Intrusion Prevention system	Per VM	1	No	
12	Cloud Monitoring Service	Per Device	1	No	
13	MS SQL Std (2 vCores/License)	Latest	1	No	
14	MS SQL Ent (2 vCores/License)	Latest	1	No	
15	Virtual Load Balancer	1 Gbps	1	No	
16	Cross Connect	Per termination	1	No	
17	Unmetered Internet Bandwidth	Unmetered per Mbps	1	Mbps	
18	DNS Entry	Per Instance	1	No	
19	Virtual UTM along with 25 SSL VPN for Desktop	1Gbps throughput	1	No	
20	Virtual Web Application Firewall	1Gbps throughput	1	No	
21	Vulnerability Assessment and	Per URL/Domain	1	No	
22	DDoS as a service	Gbps Mitigation	1	No	
23	Postgres Enterprise (Unicore)	Latest	1	No	
24	Postgres Community	Latest	1	No	
25	MY SQL Std	Latest	1	No	
26	CERT-IN Empaneled VAPT	Per Device	1	No	
27	Domain Wildcard SSL Certificate	Per Domain	1	No	
28	Domain SSL Certificate	Per Domain	1	No	
29	MY SQL Community	Latest	1	No	
30	DRM Tool	Per VM	1	No	
31	Replication link between DC and DR	Per Mbps	1	MBPS	

32	Backup Agent	Per VM	1	No	
33	EDR	Per Device	1	No	
34	SSL VPN	Per User	1	No	
35	Enterprise Email as a Service	Per Mailbox	1	No	
36	Storage Managed Services	Per TB	1	No	
37	Backup Managed Services	Per VM	1	No	
38	Archival Managed Services	Per VM	1	No	
39	vFirewall Managed Services	Per vFW	1	No	
40	vWAF Managed Services	Per vWAF	1	No	
41	vLB Managed Services	Per vLB	1	No	
42	Database Managed Services	Per 100 GB	1	No	
43	OS Managed Services	Per OS	1	No	
44	Application Performance Monitoring tool –	Per Web/App server	1	No	
45	Database Performance Monitoring Tool –	Per DB server	1	No	
46	Database activity Monitoring	Per DB instance	1	No	
47	CDN as a Service	Per TB	1	No	
48	email gateway	Per 1 Lac Email	1	No	
49	SMS gateway	Per 1 Lac SMS	1	No	
50	RHEL Small and Large Instance	Latest	1	No	
51	CENT OS	Latest	1	No	
52	Patch Management	Latest	1	No	

53	SIEM as a Service	Devices in infrastructure	1	No	
Total				**Rs.**	

All unit rates are exclusive of all applicable taxes, duties and levies, and are firm/ceiling rates for the initial contract period. Rates applicable during any extension period shall be as mutually agreed under the Extension of Contract clause.

18 Professional Resources Details

The following are minimum qualifications and experience for key resources required to implement the cloud solution. The following personnel would be required during the Configuration, Installation and Setup of the Cloud solution. The Project Manager would continue during the post implementation project management phase.

#	Role	Minimum Qualification & Experience
1	Project Manager	• B.E. / B.Tech./MCA or equivalent • PMP or equivalent certification • 10+ Years of Experience; 5+ years of Experience as Project Manager • Present experience of 2+ Years in managing a cloud-service project
2	Solution Architect	• B.E. / B.Tech. / MCA or equivalent • 5+ Years of Experience in Solution Design
3	Cloud Administrator	• B.E. / B.Tech. / MCA or equivalent • 8+ Years of Experience in Implementation, Management and Operations
4	System Administrator	• B.E. / B.Tech. / MCA or equivalent • 5+ Years of Experience in Implementation, Management and Operations
5	Network Administrator	• B.E. / B.Tech. / MCA or equivalent • 5+ Years of Experience in network provisioning, configuration and management

6	Security Administrator	• B.E. / B.Tech. / MCA or equivalent • 5+ Years of Experience in Implementation, Management and Operations of security devices and solution

CV Format: CSP has to provide the details on above mentioned resources in the below format.

CURRICULUM VITAE (CV)

<table>
<tr><td>1.</td><td colspan="2">Proposed position</td><td colspan="4"></td></tr>
<tr><td>2.</td><td colspan="2">Name of firm</td><td colspan="4"></td></tr>
<tr><td>3.</td><td colspan="2">Name of expert</td><td colspan="4">[First] [Middle] [Surname]</td></tr>
<tr><td>4.</td><td colspan="2">Date of birth</td><td colspan="4"></td></tr>
<tr><td>5.</td><td colspan="2">Nationality</td><td colspan="4"></td></tr>
<tr><td>6.</td><td colspan="2">Education</td><td colspan="4">[Indicate college/university and other specialized education of staff member, giving names of institutions, degrees obtained, and year of obtainment starting from the latest degree]</td></tr>
<tr><td>7.</td><td colspan="2">Membership of Professional Organizations</td><td colspan="4"></td></tr>
<tr><td>8.</td><td colspan="2">Training & Publications</td><td colspan="4">[Indicate significant training since education degrees (under 5) were obtained]</td></tr>
<tr><td>9.</td><td colspan="2">Countries of Work Experience</td><td colspan="4">[List countries where staff has worked in the last ten years]</td></tr>
<tr><td rowspan="5">10.</td><td rowspan="5">Languages</td><td rowspan="2">Language</td><td colspan="4">Proficiency (Good/ Fair/ Poor)</td></tr>
<tr><td>Speaking</td><td colspan="2">Reading</td><td>Writing</td></tr>
<tr><td>English</td><td></td><td colspan="2"></td><td></td></tr>
<tr><td></td><td></td><td colspan="2"></td><td></td></tr>
<tr><td></td><td></td><td colspan="2"></td><td></td></tr>
<tr><td rowspan="8">11.</td><td rowspan="8">Employment record [Starting with present position, list in reverse order every employment held by staff member since graduation]</td><td colspan="2">Name of Organization</td><td colspan="2">Position held</td><td>Duration</td></tr>
<tr><td colspan="2"></td><td colspan="2"></td><td>YYYY to present</td></tr>
<tr><td colspan="2"></td><td colspan="2"></td><td></td></tr>
<tr><td colspan="2"></td><td colspan="2"></td><td></td></tr>
<tr><td colspan="2"></td><td colspan="2"></td><td></td></tr>
<tr><td colspan="2"></td><td colspan="2"></td><td></td></tr>
<tr><td colspan="2"></td><td colspan="2"></td><td></td></tr>
<tr><td colspan="5"></td></tr>
<tr><td>12.</td><td>Details of tasks assigned</td><td colspan="4"></td></tr>
<tr><td>13.</td><td>Work Undertaken that Best Illustrates Capability to Assigned Handle the Tasks Assigned</td><td colspan="4">[Among the assignments in which the Staff has been involved, indicate the following information for those assignments that best illustrate staff capability to handle the tasks assigned.]
Name of assignment or project:
Year:
Location:
Client:</td></tr>
</table>

		Project Cost: Main project features: Positions held: Activities performed:
14.		Name of assignment or project: Year: Location: Client: Project Cost: Main project features: Positions held: Activities performed:
15.	**Certification**	I, the undersigned, certify that to the best of my knowledge and belief, this CV correctly describes me, my qualifications, and my experience. I understand that any wilful misstatement described herein may lead to my disqualification or dismissal, if engaged.

Signature	Signature
Date: [dd/mm/yyyy]	Date: [dd/mm/yyyy]
Name of expert:	Name of Authorized Signatory:

Note:

1. *Please restrict the number of pages per CV to four (04) pages (two sheets if printed both sides). The one-page summary shall be over and above the four (04) page CV. Pages in the CV greater than these limits shall not be considered for evaluation.*
2. *CVs must be signed in indelible ink by the key expert and authorized signatory of the Bidders. In case of Unsigned CVs shall be rejected.*

19 Appendices

19.1 Appendix A: Form of Bank Guarantee for Performance Security

(To be stamped in accordance with Stamp Act if any, of the country for issuing bank)

To:
Managing Director,
Maharashtra Industrial Township Limited,
Udyog Sarathi, MIDC Office,
Marol Industrial Area, Andheri (East),
Mumbai, Maharashtra State, India – 400093

WHEREAS _____[name and address of Contractor] (hereinafter called "the Contractor") has undertaken, in pursuance of Contract No. _____ dated _____ to execute **"RFP for Selection of Service Provider (Cloud Hosting and Managed Service) to Setup, Migrate, and Manage Data Centre (DC) and Disaster Recovery (DR) site for MITL on Cloud"** (hereinafter called "the Contract"). AND WHEREAS it has been stipulated by you in the said Contract that the Contractor shall furnish you with a Bank Guarantee by a nationalised/schedule bank in India for the sum specified therein as security for compliance with its obligations in accordance with the Contract.

AND WHEREAS we have agreed to give the contractor such a Bank Guarantee;

NOW THEREFORE we agree unconditionally and irrevocably to guarantee as primary obligator and not as Surety merely, on behalf of the contractor, a total of upto _____ [amount of Guarantee] _____ [in words], such sum being payable in the types and proportion of currencies in which the Contract Price is payable, and we undertake to pay you, upon first written demand and without cavil or argument, any sum or sums within the limits of _____ [amount of Guarantee] as aforesaid without your needing to prove or to show grounds or reasons for your demand for the sum specified therein.

We hereby waive the necessity of your demanding the said debt from the Contractor before presenting us with the demand.

We further agree that no change or addition to or other modification of the terms of the Contract or of the Works to be performed there under or of any of the Contract documents which may be made between you and the Contractor shall in any way release us from any liability under this guarantee, and we hereby waive notice of any such change, addition or modification.

This guarantee shall be valid until …….(the end of warranty period of 2 years).

Notwithstanding anything to the contrary contained herein-

i. Our liability under this Guarantee shall not exceed Rs…….. (Rupees …….)

ii. This Bank Guarantee shall remain valid up to ……..(expiry date of Bank Guarantee); and

iii. We are liable to pay up to the guarantee amount only and only if we receive from you a written claim or demand not later than ……. (claim period should be further one year after the expiry date). All your

rights as well as our liability under this Bank Guarantee shall stand extinguished unless a written claim or demand is made under this guarantee on …….(Bank address in Mumbai, Maharashtra) not later than claim period should be further one year after the expiry date.

Signature and Seal of the Guarantor_____

Name of Bank _____

Address _____

Date _____

19.2 DRAFT MASTER SERVICE AGREEMENT

THIS SERVICE LEVEL AGREEMENT AND CONTRACT (hereinafter referred to as the "Agreement") is entered into on this _____ day of _____, 2026 (the "Effective Date").

BY AND BETWEEN:

Maharashtra Industrial Township Limited, a company incorporated under the laws of India, having its principal place of business at [Insert Office Address] (hereinafter referred to as **"MITL"** or the **"Purchaser"**, which expression shall, unless repugnant to the context, include its successors and permitted assigns) of the FIRST PART;

AND:

[Insert Selected Bidder's Legal Name], an empanelled Cloud & Managed Service Provider, registered under the Companies Act, [1956/2013], having its registered office at [Insert Provider Address] (hereinafter referred to as the **"Service Provider"**, which expression shall, unless repugnant to the context, include its successors and permitted assigns) of the SECOND PART.

(Each of the parties shall individually be referred to as a "Party" and collectively as the "Parties".)

1. DEFINITIONS & INTERPRETATION

"GCC" means Government Community Cloud infrastructure empanelled by MeitY.

"Managed Services" means end-to-end operation, administration, security monitoring, optimisation, patch management, and backup of the cloud environments.

"SLA" means Service Level Agreement stipulating performance indicators, uptime parameters, and financial penalties for default.

2. SCOPE OF WORK

2.1. The Service Provider shall deliver comprehensive "Government Community Cloud (GCC) Hosting and Complete Managed Services" for MITL's core business applications as stipulated in the Tender No.-

2.2. The deployment model shall be a secure, logically isolated Government Community Cloud environment complying strictly with MeitY directives.

3. TERM AND EXTENSION

- **Months 2: Commencement of Services —** Signing of the MSA, setup of the GCC landing zone, application migration, testing, and formal sign-off.
- **Months 24: Core Contractual Period —** The baseline contract runs for a fixed period of twenty-four (24) months, governed by the monthly/quarterly SLA performance monitoring.
- **Post-Month 26: Mutual Extension Window —** The contract may be extended based on mutual written agreement between MITL and the Service Provider, subject to satisfactory performance.
- **Contract End: Mandatory Exit Management —** A 90-day transition period where the Service Provider hands over all data, backups, and configurations to MITL without extra friction or lock-in fees.

4. DATA SOVEREIGNTY, PRIVACY, AND SECURITY

4.1. Localization: The Service Provider explicitly warrants that all primary data, secondary database copies, system metadata, event logs, and backups shall reside physically within the geographic boundaries of India.

4.2. DPDP Act Compliance: The Service Provider must process any personal data strictly in compliance with the Digital Personal Data Protection (DPDP) Act. The Service Provider shall deploy appropriate technical and organizational measures to ensure immediate data breach reporting to MITL within a maximum of two (2) hours of discovery.

4.3. Access Control: No data hosted under this contract shall be transferred, replicated, or made accessible to any foreign government, cross-border entity, or third-party subcontractor without explicit written authorization from MITL.

5. SERVICE LEVEL AGREEMENT (SLA) & PENALTIES

The Service Provider shall maintain the following minimum infrastructure availability benchmarks. SLA metrics will be reviewed monthly, As per the terms and conditions mentioned in the tender documents

6. CONSIDERATION AND PAYMENT TERMS

6.1. MITL shall pay the Service Provider in accordance with the discovered financial bid rates, as per the pay and used module.

6.2. Payments will be released on a Quarterly basis upon submission of clean, undisputed invoices accompanied by verified SLA compliance reports generated by automated monitoring tools.

6.3. All payments are subject to tax deductions at source (TDS) as per applicable Indian fiscal regulations.

7. TERMINATION

7.1. For Convenience: MITL reserves the right to terminate this contract by giving ninety (90) days advance written notice to the Service Provider without assigning any reason.

7.2. For Default: If the Service Provider fails to cure an SLA breach or operational deficiency within fifteen (15) days of receiving a written notice from MITL, MITL may terminate the contract immediately with zero financial liability.

8. INTELLECTUAL PROPERTY RIGHTS (IPR)

All source code, database structures, business data, analytics, configuration setups, and proprietary application frameworks hosted on the provided infrastructure shall remain the absolute, exclusive intellectual property of MITL. The Service Provider shall claim no lien, right, or ownership over MITL data under any circumstances.

9. DISPUTE RESOLUTION AND JURISDICTION

9.1. Any dispute, difference, or controversy arising out of this contract shall be referred to amicable resolution through mutual discussions between senior executives of both organizations.

9.2. If unresolved within thirty (30) days, the dispute shall be referred to arbitration in accordance with the Arbitration and Conciliation Act, 1996. The seat and venue of arbitration shall be Mumbai, Maharashtra, India.

9.3. This agreement shall be governed by the laws of India, and the courts at [Insert City] shall hold exclusive jurisdiction.

IN WITNESS WHEREOF, the Parties hereto have caused this Agreement to be executed by their respective authorized representatives as of the Effective Date first written above.

For and on behalf of MITL (Purchaser)	**For and on behalf of Service Provider**
Signature: _____	Signature: _____
Name: _____	Name: _____
Designation: _____	Designation: _____
Date: _____	Date: _____

Witness 1: _____ (Name, Address, & Signature)

Witness 2: _____ (Name, Address, & Signature)

19.3 Format Submission of Pre-Bid Query

The Bidder shall submit its queries/clarifications related to this RFP to the Employer in the prescribed format given below, through the email ID specified in the RFP.

Name of the Work: **"FP for Selection of Service Provider (Cloud Hosting and Managed Service) to Setup, Migrate, and Manage Data Centre (DC) and Disaster Recovery (DR) site for MITL on Cloud."**

Sr.No.	RFP Reference (Section / Page)	Provision as per RFP	Query / Clarification Sought	Employer Response