RAILTEL CORPORATION OF INDIA LIMITED

(A Govt. of India Undertaking)

Expression of Interest for Selection of Partner from Empaneled Business Associate/ Channel Partners/ System Integrators

For

"Provisioning, Configuration, Testing, Commissioning, Operations & Maintenance of Cloud Services for BMC"

EOI No: RCIL/WR/MUMBAI/Mktg/25-26/10 dated 13th June, 2025

EOI NOTICE

RailTel Corporation of India Ltd,
Western Railway Microwave Complex, Senapati Bapat Marg,
Mahalaxmi, Mumbai – 400013

EOI Notice No: RCIL/WR/MUMBAI/Mktg/25-26/10

RailTel Corporation of India Ltd., (here after referred to as "RailTel") invites EOIs from RailTel's Empaneled Partners/ Business Associates/ Channel Partners/ System Integrators for "Provisioning, Configuration, Testing, Commissioning, Operations & Maintenance of Cloud Services for BMC" as per Brihanmumbai Municipal Corporation's Bid No: 2025_MCGM_1182423_1 dated 29.05.2025 and any other addendums/corrigendum/documents contained within and related to the same.

The details are asunder:

1	Last date for submission of Technical Packet against EOIs by bidders	17th June 2025 at 15:00 Hours
2	Opening of Technical Bid of EOIs	17th June 2025 at 15:30 Hours
3	Number of copies to be submitted for scope of work	One
4	EOI fees inclusive tax (Non-refundable)	Rs. 35,695 /-
5	EMD (Token EMD)	Rs. 1,16,89,351 /- in the form of online transfer as EMD along with submission of EoI response.

The EMD should be in the favor of RailTel Corporation of India Limited payable at Mumbai through online bank transfer. Partner needs to share the online payment transfer details like UTR No, date of payment, etc.

RailTel Bank Details: Union Bank of India, **Account No**. 317801010036605, **IFSC Code** - UBIN0531782.

Eligible Business Associates are required to direct all communications related to this Invitation for EoI document, through the following Nominated Point of Contact persons:

1. Level 1
Contact Name: Sh. Saish Sankhe
Designation: Deputy Manager/Marketing
E-Mail Address: saish.sankhe@railtelindia.com
Mobile No: +91-8999292981

2. Level 2
Contact Name: Sh. Viplov Nath Mishra
Designation: Senior Deputy General Manager/ Marketing
E-Mail Address: viplovmishra@railtelindia.com
Mobile No: +91- 90044 44124

Note:

1. Empaneled partners are required to submit soft copy of technical packet through an e-mail at **eoi.wr@railtelindia.com** duly signed by Authorized Signatories with Company seal and stamp.
2. The EOI response is invited from eligible **Empaneled Partners of RailTel only.**
3. All the documents must be submitted with **proper indexing** and **page no**.
4. This is a **post partnership arrangement with empaneled business associate of RailTel for execution of end customer RFP**. Selected partner's authorized signatory has to give an undertaking they will not submit directly or indirectly their bids and techno-commercial solution/association with any other organization once selected in this EOI for post-bid teaming arrangement (before and after submission of bid to end customer organization by RailTel). This undertaking has to be given with this EOI Response.
5. Partner has to submit their response as an individual organization only. No consortium is allowed. The Bidder has to be an empaneled partner of RailTel.
6. **Transfer and Sub-letting**. The Business Associate has no right to give, bargain, sell, assign or sublet or otherwise dispose of the Contractor any part thereof, as well as to give or to let a third party take benefit or advantage of the present Contract or any part thereof.
7. All Bidders to sign and stamp RailTel's EOI and its corrigendum's implying acceptance of all terms and conditions as mentioned and submit the same along with their Bids.

1. Introduction about RailTel

RailTel Corporation of India Limited (RailTel), an ISO-9001:2000 organization is a Mini Ratna Government of India undertaking under the Ministry of Railways. The Corporation was formed in Sept 2000 with the objectives to create nationwide Broadband Telecom and Multimedia Network in all parts of the country, to modernize Train Control Operation and Safety System of Indian Railways and to contribute to realization of goals and objective of national telecom policy 1999. RailTel is a wholly owned subsidiary of Indian Railways.

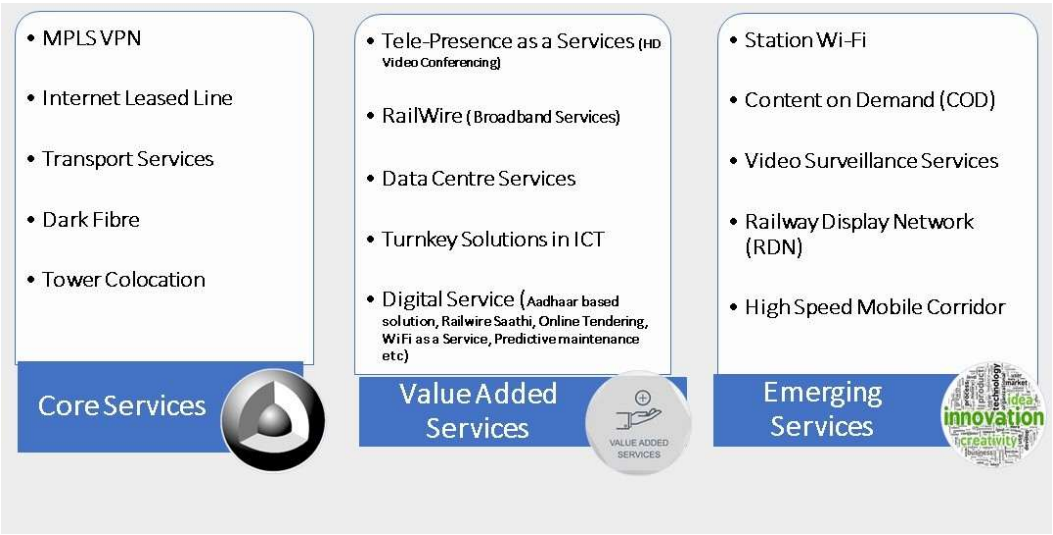
RailTel has approximately 60000 kms of OFC along the protected Railway tracks. The transport network is built on high capacity DWDM and an IP/ MPLS network over it to support mission critical communication requirements of Indian Railways and other customers. RailTel has Tier-III Data Center in Gurgaon and Secunderabad hosting / collocating critical applications. RailTel is also providing Telepresence as a Service (TPaaS), where a High-Definition Video Conference facility bundled with required BW is provided as a Service.

For ensuring efficient administration across India, country has been divided into four regions namely, Eastern, Northern, Southern & Western each headed by Executive Director and Headquartered at Kolkata, New Delhi, Secunderabad & Mumbai respectively. These regions are further divided into territories for efficient working. RailTel has territorial offices at Guwahati, & Bhubaneswar in East, Chandigarh, Jaipur, Lucknow in North, Chennai & Bangalore in South, Bhopal, and Pune & Ahmedabad in West. Various other territorial offices across the country are proposed to be created shortly.

RailTel's business service lines can be categorized into three heads namely B2G/B2B (Business to Government and Business to Business) and B2C (Business to customers):

Licenses & Service portfolio:

Presently, RailTel holds Infrastructure Provider -1, National Long Distance Operator, International Long Distance Operator and Internet Service Provider (Class-A) licenses under which the following services are being offered to various customers:



a) **Carrier Services**

- National Long Distance: Carriage of Inter & Intra -circle Voice Traffic across India using state of the art NGN based network through its Interconnection with all leading Telecom Operators
- Lease Line Services: Available for granularities from E1 to multiple of Gigabit bandwidth & above.
- Dark Fiber/Lambda: Leasing to MSOs/Telco's along secured Right of Way of Railway tracks.
- Co-location Services: Leasing of Space and 1000+ Towers for collocation of MSC/BSC/BTS of Telco's

b) **Enterprise Services**

- Managed Lease Line Services: Available for granularities from E1, DS-3, STM-1 & above
- MPLS VPN: Layer-2 & Layer-3 VPN available for granularities from 2 Mbps& above
- Dedicated Internet Bandwidth: Experience the "Always ON" internet connectivity at your fingertips in granularities 2 Mbps to several Gbps.

c) **DATA CENTER**

- Infrastructure as a service (IaaS), Hosting as Services, Security operation Centre as a Service (SOCaaS): RailTel has MeitY empaneled two Tier-III data centres in Gurgaon & Secunderabad. Presently RailTel is hosting critical applications of Indian Railways, Central & State government/ PSUs applications. RailTel will facilitate Government's applications
- Hosting services including smooth transition to secured state owned RailTel's Data Centers and Disaster Recovery Centres. RailTel also offers SOC as a Service 'SOCaaS'. In addition, RailTel offers VPN client services so that employees can seamlessly access government's intranet, applications securely from anywhere without compromising security.

d) **National Long Distance:**

Carriage of Inter & Intra -circle Voice Traffic across India using state of the art NGN based network through its Interconnection with all leading Telecom Operators

- Lease Line Services: Available for granularities from E1 to multiple of Gigabit bandwidth & above
- Dark Fiber/Lambda: Leasing to MSOs/Telco's along secured Right of Way of Railway tracks
- Co-location Services: Leasing of Space and 1000+ Towers for collocation of MSC/BSC/BTS of Telco's

e) High-Definition Video Conference:

RailTel has unique service model of providing high-definition video conference bundled with Video Conference equipment, bandwidth and FMS services to provide end-to-end seamless services on OPEX model connecting HQ with other critical offices. RailTel also offers application-based video conference solution for employees to be productive specially during this pandemic situation.

f) Retail Services – RailWire

RailWire: Triple Play Broadband Services for the Masses. RailTel has unique model of delivering broadband services, wherein local entrepreneurs are engaged in delivering & maintaining broadband services and upto 66% of the total revenues earned are shared to these local entrepreneurs in the state, generating jobs and revitalizing local economies. On date RailTel is serving approx. 4,68,000 subscribers on PAN Indian basis. RailTel can provide broadband service across– Government PSU or any organization's officers colonies and residences.

2. Project Background and Objective of EOI

RailTel intends to participate in RFP floated by end Customer organization, Brihanmumbai Municipal Corporation for "Provisioning, Configuration, Testing, Commissioning, Operations & Maintenance of Cloud Services for BMC" with RFB No: 2025_MCGM_1182423_1 dated 29.05.2025.

RailTel invites EOIs from RailTel's Empaneled Partners / Business Associates/ Channel partners/ System Integrators for the selection of suitable partner for participating in above mentioned work for the agreed scope work. The empaneled partner is expected to have excellent execution capability and good understanding customer local environment.

3. Scope of Work

In accordance with the BMC RFB No: 2025_MCGM_1182423_1 dated 29.05.2025, BMC seeks to select single MSP to provide Cloud services for the contract duration mentioned in the customer RFP for Provisioning, Configuring, Testing, Commissioning, Operating and Maintaining the Cloud Services

The detailed scope of work can be referred from the end customer tender.

Special Note: RailTel may retain some portion of the work mentioned in the end organization RFP, where RailTel has competence so that overall proposal becomes most winnable proposal.

4. Response to EOI guidelines

4.1 Language of Proposals

The proposal and all correspondence and documents shall be written in English in soft copy through an email.

4.2 RailTel's Right to Accept/Reject responses

RailTel reserves the right to accept or reject any response and annul the bidding process or even reject all responses at any time prior to selecting the partner, without thereby incurring any liability to the affected bidder or Business Associate or without any obligation to inform the affected bidder or bidders about the grounds for RailTel's action.

4.3 EOI response Document

The bidder is expected to examine all instructions, forms, terms and conditions and technical specifications in the bidding documents. Submission of bids, not substantially responsive to the bidding document in every aspect will be at the bidder's risk and may result in rejection of its bid without any further reference to the bidder.

All pages of the documents shall be signed by the bidder including the closing page in token of his having studies the EOI document and should be submitted along with the bid.

4.4 Period of Validity of bids and Bid Currency

Bids shall remain valid for a period of 120 days from the date Bid submission date issued by the end Customer organization for which bid is going to submit.

4.5 Bid Earnest Money (EMD)

4.5.1 The Business Associate shall furnish a sum as given in EOI Notice via online transfer from any bank in India in favour of "RailTel Corporation of India Limited" along with the offer. This will be called **EOI EMD.**

4.5.2 Offers not accompanied with valid EOI Earnest Money Deposit shall be summarily rejected. EMD if paid via online transfer then the details of the payment (UTR No, Payment Date, etc) should be accompanied along with the bid.

4.5.3 In case if offer is selected for bidding, the partner has to furnish Earnest Money Deposit (for balance amount as mentioned in the customer's Bid or as applicable) for the bid to RailTel. The selected Business Associate shall have to transfer the balance EMD in proportion to the quoted value/scope of work to RailTel before RailTel's submission of bid to end customer as applicable.

4.5.4 **Return of EMD for unsuccessful Business Associates:** EOI EMD of the unsuccessful Business Associate shall be returned without interest after completion of EOI process.

4.5.5 **Return of EMD for successful Business Associate:** EOI-EMD & Earnest Money Deposit (balance proportionate EMD) if applicable and Integrity Pact BG of the successful bidder will be discharged / returned as promptly as possible after the receipt of RailTel's EMD/BG from the Customer and or on receipt of Security Deposit Performance Bank Guarantee as applicable (clause no. 4.6) from Business Associate whichever is later.

4.5.6 **Forfeiture of EOI EMD or EOI EMD & EMD (balance proportionate EMD) and or Penal action asper EMD Declaration**:

The EMD may be forfeited and or penal action shall be initiated if a Business Associate withdraws his offer or modifies the terms and conditions of the offer during the validity period.

- In case of non-submission of SD/PBG (as per clause no. 4.6) lead to forfeiture of EMD and Integrity Pact and or suitable action as prescribed in the EMD Declaration shall be initiated as applicable.
- Having participated with another party/consortium apart from RailTel in RailTel's end customer Tender.
- Partial or non-submission of EMD/Tender Fees or both.

4.6 Security Deposit / Performance Bank Guarantee (PBG)

In case the bid is successful, the PBG of requisite amount proportionate to the agreed scope of the work will have to be submitted to RailTel.

As per work share arrangements agreed between RailTel and Business Associate the PBG will be proportionately decided and submitted by the selected Business Associate.

4.7 Last date & time for Submission of EOI response

EOI response must be submitted to RailTel at the email address specified in the preamble not later than the specified date and time mentioned in the preamble.

4.8 Modification and/or Withdrawal of EOI response

EOI response once submitted will be treated as final and no modification will be permitted except with the consent of the RailTel.

No Business Associate shall be allowed to withdraw the response after the last date and time for submission.

The successful Business Associate will not be allowed to withdraw or back out from the response commitments. In case of withdrawal or back out by the successful business associate, the Earnest Money Deposit shall be forfeited, and all interests/claims of such Business Associate shall be deemed as foreclosed.

4.9 Details of Financial bid for the above referred tender

Business Associate meeting eligibility criteria will be selected for optimizing technical and commercial solution so that most winnable solution is submitted to end customer.

In case if there are Two or more Business Associate meeting eligibility criteria, all bidders will get empaneled. A price bid will be called later after the tender is floated by the customer. The final bid for the tender will be prepared jointly with the selected Business Associate so that the optimal bid can be put with a good chance of winning the Tender.

4.10 Clarification of EOI Response

To assist in the examination, evaluation and comparison of bids the purchaser may, at its discretion, ask the Business Associate for clarification. The response should be in writing and no change in substance of the EOI response shall be sought, offered or permitted.

4.11 Period of Association/Validity of Agreement

RailTel will enter into an agreement with selected bidder with detailed Terms and conditions.

5. Eligibility Criteria for Bidding Business Partner of RailTel

S No	Particulars	Criteria for Tender Package (Mandatory Compliance & Document Submission)
A)	**Financial Conditions**	
i)	Sole bidder should be registered under Companies Act, 1956 or Companies Act 2013 or Limited Liability partnership act 2008 as amended and should have at least 3 years of operations in India as on bid submission date.	1. Certificate of Incorporation 2. MOA and AOA 3. GST Registration 4. PAN Card 5. Documentary proof for operations in India for a period of at least 3 years as on date of publication of bid.
ii)	Sole Participating bidder should have cumulative annual turnover of at least INR **75 Cr** for last three Financial years (FY 21-22, 22-23, 23-24).	1. Turnover Certificate issued by the Chartered Accountant for sole bidder. Certificate should contain UDIN no. issued by ICAI
iii)	Sole partner should also have positive net worth & be profitable in the last financial year (i.e. FY 23-24).	1. Positive Net Worth and Profitability Certificate issued by the CA for the last financial year (i.e. FY 24-25). Certificate should contain UDIN no. issued by ICAI.
B)	**Technical Conditions**	
iv)	The Bidder must have experience of successful migration and / or management of Cloud / **Data Center** project(s) during last five years (as on the last date of bid submission) in Central / State Government/ Urban Local Bodies / Public Sector Companies / Banking Financial Services & Insurance (BFSI)/ Private Sector of below mentioned project value in India: Project shall include setting up & hosting of IT infrastructure &	Form Specific Experience along with Completion certificates from the client; OR Work order + Self certificate of completion (Certified by the statutory auditor / Chartered Accountant); OR Work Order + Phase Completion Certificate from the client Bidder should also submit a certification from the client confirming the value of the project.

	systems at Data Center /Cloud/ Private cloud / Infrastructure as a Service (IaaS) or Platform as a Service (PaaS) for contracts involving provisioning, testing, and operations & maintenance of Cloud / Data Center Services 1. At least one project with a value not less than ~~48~~ 24 Crore OR 2. At least two projects with a value not less than ~~35~~ 17 Crore OR 3. At least three projects with a value of not less than ~~24~~ ~~12~~ Crore	
v)	The CSP should be a MeitY/ MahaIT/ DIT Empaneled Cloud Service Provider (CSP)	Undertaking from the bidder on the letter head of the company, mentioning that CSP is a MeitY Empaneled and STQC Audit Compliant. And/or MeitY empaneled letter with validity.
vi)	The bidder must have strength of at least 50 IT Professionals (data center/networking/system administration/cloud services / cloud security, maintenance of cloud solution/ virtual server administration/system administration, database etc) on their payroll as on date of submission of this bid. At least 10 of these professionals must have certification(s) in Cloud expertise areas.	Self-declaration from the Authorized signatory of the Bidder on their letterhead
C)	**CSP Documents**	
vii)	CSP must have the following certifications: - ISO 27001, ISO 27017, ISO 27018	Copy of the Valid Certificate signed and stamped by the Authorized Signatory of the CSP.
viii)	CSP should have accreditations. Relevant to security, availability, confidentiality, processing integrity, and/or privacy Trust Services principles. SOC 1, SOC 2, SOC 3 and PCI DSS	Self-declaration from the Authorized signatory of the CSP on their letterhead
ix)	The Bidder must provide OEM MAF for all the solutions provided.	Signed and stamped MAF by OEM to be provided

6. Bidder's Profile

The bidder shall provide the information in the below table:

S. No.	ITEM	Details
1.	Full name of bidder's firm	

2.	Full address, telephone numbers, fax numbers, and email address of the primary office of the organization / main / head / Corporate office	
3.	Name, designation and full address of the Chief Executive Officer of the bidder's organization as a whole, including contact numbers and email Address	
4.	Full address, telephone and fax numbers, and email addresses of the office of the organization dealing with this tender	
5.	Name, designation and full address of the person dealing with the tender to whom all reference shall be made regarding the tender enquiry. His/her telephone, mobile, Fax and email address	
6.	Bank Details (Bank Branch Name, IFSC Code, Account number)	
7.	GST Registration number	

7. Evaluation Criteria

7.1 The Business Associates are first evaluated on the basis of the Eligibility Criteria as per clause 5 above.

7.2 The Business Associate qualifying the Eligibility criteria will be selected for optimizing technical and commercial solution so that most winnable solution is submitted to end customer.

7.3 In case if there are two or more Sole Bidders meeting eligibility criteria then all bidders meeting the eligibility criteria will be empaneled. Price bids will be sought from these Sole Bidders in a later stage after the Customer tender is floated and Sole Bidder with overall lowest (L1) offer will be selected for optimizing technical and commercial solution.

7.4 RailTel reserves the right to accept or reject the response against this EOI, without assigning any reasons. The decision of RailTel is final and binding on the participants. The RailTel evaluation committee will determine whether the proposal/ information is complete in all respects and the decision of the evaluation committee shall be final. RailTel may at its discretion assign lead factor to the Business associate as per RailTel policy for shortlisting partner against this EOI.

7.5 All General requirements mentioned in the Technical Specifications are required to be complied. The solution proposed should be robust and scalable.

8 Withdrawal of Bids

A Bidder wishing to withdraw its bid shall notify to RailTel by e-mail prior to the deadline prescribed for bid submission. The notice of withdrawal shall be addressed to RailTel at the address named in the Bid Data Sheet, and bear the Contract name, the <Title> and < Bid No.>, and the words "Bid Withdrawal Notice." Bid withdrawal notices received after the bid submission deadline will be ignored, and the submitted bid will be deemed to be a valid submitted bid.

No bid can be withdrawn in the interval between the bid submission deadline and the expiration of the bid validity period specified in the Bid Data Sheet. Withdrawal of a bid during this interval may result in the forfeiture of the Bidder's EMD.

9 Evaluation Process

The evaluation process of the bid proposed to be adopted by RailTel is indicated in this section. The purpose of this section is to provide the Bidder an idea of the evaluation process that

RailTel may adopt.

RailTel shall appoint a Bid Evaluation Committee (BEC) to scrutinize and evaluate the technical and commercial bids received. The BEC will examine the Bids to determine whether they are complete, responsive and whether the bid format conforms to the bid requirements. RailTel may waive any informality or non-conformity in a bid which does not constitute a material deviation according to RailTel.

The bid prices should not be mention in any part of the bid other than the Commercial Bid. Any attempt by a bidder to influence the bid evaluation process may result in the rejection of Bid and forfeiture of EMD.

10 Performance Bank Guarantee

The Bidder shall at his own expense, deposit with RailTel, an unconditional and irrevocable Performance Bank Guarantee (PBG) from nationalized banks as per the format given in this bid, payable on demand, for the due performance and fulfilment of the contract by the Bidder.

This Performance Bank Guarantee will be submitted within 21 days of the notification of award of the contract/ Letter of Acceptance (LOA) issuance whichever is earlier. If PBG is not submitted within this time frame a delayed PBG penalty will be attracted. Post 21 days and upto 60 days from date of notification of award of the contract/ Letter of Acceptance (LOA) issuance a penalty at 15% per annum interest of LOA amount will be levied as delayed PBG penalty and this penalty will be deducted from the Invoices & EMD of the Bidder. After these 60 days if PBG is not submitted then it will be assumed that the Bidder is not interested in submitting PBG and the Amount of PBG along with the delayed PBG penalty calculated will be retained from Invoices & EMD of the Bidder. Non submission of PBG can also lead to cancellation of contract and the decision with respect to whether, to retain the PBG Amount and penalty from Invoices & EMD or cancellation of contract, will be at the sole discretion of RailTel. In the event of cancellation of contract EMD will be forfeited. If PBG is retained from Invoices & EMD then the PBG Amount only and not the penalty attracted will be paid to the Bidder in such a case post the contract period plus three months (expected PBG validity date) are over after deducting any applicable deductions (eg: Poor service, etc).

This Performance Bank Guarantee will be for an amount equivalent to 5% of the total contract value. All charges whatsoever such as premium, commission, etc. with respect to the Performance Bank Guarantee shall be borne by the Bidder. The Performance Bank Guarantee format can be found in this document.

The Performance Bank Guarantee may be discharged/ returned by RailTel upon being satisfied that there has been due performance of the obligations of the Bidder under the contract. However, no interest shall be payable on the Performance Bank Guarantee.

In the event of the Bidder being unable to service the contract for whatever reason, RailTel would invoke the PBG. Notwithstanding and without prejudice to any rights whatsoever of RailTel under the Contract in the matter, the proceeds of the PBG shall be payable to RailTel as compensation for any loss resulting from the Bidder's failure to complete its obligations under the Contract. RailTel shall notify the Bidder in writing of the exercise of its right to receive such compensation within 30 days, indicating the contractual obligation(s) for which the Bidder is in default.

The 30 days' notice period shall be considered as the 'Cure Period' to facilitate the Implementation Agency to cure the breach. The PBG shall be invoked only if the breach is solely attributable to the bidder and the bidder fails to rectify the breach within the 'Cure Period'.

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

11 Rights to Terminate the Process

RailTel may terminate the bid process at any time and without assigning any reason. RailTel makes no commitments, express or implied, that this process will result in a business transaction with anyone.

This bid document does not constitute an offer by RailTel. The Bidder's participation in this process may result in RailTel selecting the Bidder to engage in further discussions and negotiations towards execution of a contract. The commencement of such negotiations does not, however, signify a commitment by RailTel to execute a contract or to continue negotiations. RailTel may terminate negotiations at any time without assigning any reason.

12. Payment terms

12.1 RailTel shall make payment to selected Business Associate after receiving payment from Customer for the agreed scope of work. In case of any penalty or deduction made by customer for the portion of work to be done by BA, same shall be passed on to Business Associate.

12.2 All payments by RailTel to the Partner will be made after the receipt of payment by RailTel from end customer organization and upon submission of correct Tax Invoices as per statutory norms.

12.3 The Payments received from end customer will be disbursed Scope wise to the selected BAs. The BA selected for a particular scope will receive payments once end customer releases payments for the specific scope.

13 SLA

The selected bidder will be required to adhere to the SLA matrix as defined in the end Customer organization tender for his scope of work and the SLA breach penalty will be applicable proportionately on the selected bidder, as specified in the end Customer organization Tender. The SLA scoring and penalty deduction mechanism for in-scope of work area shall be followed as specified in the Tender. All associated clarifications, responses to queries, revisions, addendum and corrigendum, associated Prime Services Agreement (PSA)/ MSA/ SLA also included. Any deduction by Customer from RailTel payments on account of SLA breach which is attributable to Partner will be passed on to the Partner proportionately based on its scope of work.

Note:

1. **Depending on RailTel's business strategy RailTel may choose to work with Partner who is most likely to support in submitting a winning bid.**
2. **All Documents and requirements like EMD, Tender Fees, PBG, Contract Agreement to be shared/executed Back-to-Back as per the end customer RFP.**
3. **In case of any discrepancy or ambiguity in any clause /specification pertaining to scope of work area, the RFP released by end customer organization shall supersede and will be considered sacrosanct. (All associated clarifications, response to queries, revisions, addendum and corrigendum, associated prime service agreement (PSA)/ MSA/ SLA also included.)**
4. **All clauses such as cost involved, payment term, validity, lock in period, etc will be back-to-back as per RFP/ Tender.**
5. **All required MAFs are to be arranged by Selected Bidders before RailTel's submission of Bid in end customer tender.**

Annexure 1: Format for COVERING LETTER (to be submitted by sole Bidder)

COVERING LETTER (To be on company letter head)

EoI Reference No:_____Date: _____

To,

RailTel Corporation of India Ltd.
Western Railway Microwave complex,
Senapati Bapat Marg, Mahalaxmi, Mumbai – 400013

Dear Sir,

SUB: Participation in the EoI process

Having examined the Invitation for EoI document bearing the reference number _____Dt._____released by your esteemed organization, we, undersigned, hereby acknowledge the receipt of the same and offer to participate in conformity with the said Invitation for EoI document.

If our application is accepted, we undertake to abide by all the terms and conditions mentioned in the said Invitation for EoI document.

We hereby declare that all the information and supporting documents furnished as a part of our response to the said Invitation for EoI document, are true to the best of our knowledge. We understand that in case any discrepancy is found in the information submitted by us, our EoI is liable to be rejected.

We hereby Submit EMD amount of Rs._____issued vide_____from Bank _____.

Authorized Signatory Name:
Designation:
Signature:
Seal of the Organization:

Annexure 2: Format for Self-Certificate & Undertaking (to be submitted by sole Bidder)

Self-Certificate (To be on company letter head)

EoI Reference No:_____Date: _____

To,

RailTel Corporation of India Ltd.
Western Railway Microwave complex,
Senapati Bapat Marg, Mahalaxmi, Mumbai – 400013

Dear Sir,

Sub: Self Certificate for Tender, Technical & other compliances

1. Having examined the technical specifications mentioned in this EOI & end customer tender, we hereby confirm that we meet all specification.
2. We agree to abide by all the technical, commercial & financial conditions of the end customer RFP for which EOI is submitted (except pricing, termination & risk purchase rights of the RailTel). We understand and agree that RailTel shall release the payment to selected sole partner/lead partner after the receipt of corresponding payment from end customer by RailTel. Further we understand that in case selected sole bidder fails to execute assigned portion of work, then the same shall be executed by RailTel through third party or departmentally at the risk and cost of selected sole partner bidder.
3. We agree to abide by all the technical, commercial & financial conditions of the end customer's RFP for the agreed scope of work for which this EOI is submitted.
4. We hereby agree to comply with all OEM technical & Financial documentation including MAF, Technical certificates/others as per end-to-end requirement mentioned in the end customer's RFP. We are hereby enclosing the arrangement of OEMs against each of the BOQ item quoted as mentioned end customer's RFP. We also undertake to submit MAF and other documents required in the end Customer organization tender in favour of RailTel against the proposed products.
5. We hereby certify that any services, equipment and materials to be supplied are produced in eligible source country complying with OM/F. No. 6/18/2019 dated 23rd July 2020 issued by DoE, MoF.
6. We hereby undertake to work with RailTel as per end customer's RFP terms and conditions. We confirm to submit all the supporting documents constituting/ in compliance with the Criteria as required in the end customer's RFP terms and conditions like technical certificates, OEM compliance documents.
7. We understand and agree that RailTel is intending to select a sole bidder who is willing to accept all terms & conditions of end customer organization's RFP for the agreed scope of work. RailTel will strategies to retain scope of work where RailTel has competence.

8. We hereby agree to submit that in case of being selected by RailTel as sole bidder for the proposed project (for which EOI is submitted), we will submit all the forms, appendix,

relevant documents etc. to RailTel that is required and desired by end Customer well before the bid submission date by end customer and as and when required.

9. We hereby undertake to sign Agreement, Pre-Contract Integrity Pact and Non-Disclosure Agreement with RailTel on a non-judicial stamp paper of Rs. 500/- in the prescribed Format.
10. We undertake that we will not submit directly or indirectly our bids and techno-commercial solution/association with any other organization once selected in this EOI (before and after submission of bid to RailTel)

Authorized Signatory Name:
Designation:
Signature:
Seal of the Organization:

Annexure 3: Undertaking for not Being Blacklisted/Debarred (to be submitted by sole bidder)

EoI Reference No:_____Date: _____

To,

RailTel Corporation of India Ltd.
Western Railway Microwave complex,
Senapati Bapat Marg, Mahalaxmi, Mumbai – 400013

Dear Sir,

Subject: Undertaking for not being Blacklisted/Debarred

We, <Company Name>, having its registered office at <Address> hereby declares that that the Company has not been blacklisted/debarred by any Governmental/ Non-Governmental organization in India for past 3 Years as on bid submission date.

Authorized Signatory Name:
Designation:
Signature:
Seal of the Organization:

Annexure 4: Format of Affidavit (to be submitted by sole bidder)

FORMAT FOR AFFIDAVIT TO BE UPLOADED BY SOLE PARTNER ALONGWITH THE EOI DOCUMENTS

(To be executed in presence of public notary on non-judicial stamp paper of the value of Rs. 500/-. The paper has to be in the name of the BA) **

I……. (Name and designation) * appointed as the attorney/authorized signatory of the BA (including its constituents),
M/s _____(hereinafter called the BA) for the purpose of the EOI documents for the work of _____ as per the EOI No._____Dt. _____of (RailTel Corporation of India Ltd.), do hereby solemnly affirm and state on the behalf of the BA including its constituents as under:

1. I/we the BA (s), am/are signing this document after carefully reading the contents.
2. I/we the BA(s) also accept all the conditions of the EOI and have signed all the pages in confirmation thereof.
3. I/we hereby declare that I/we have downloaded the EOI documents from RailTel website www.railtelindia.com. I/we have verified the content of the document from the website and there is no addition, no deletion or no alternation to be content of the EOI document. In case of any discrepancy noticed at any stage i.e., evaluation of EOI, execution of work or final payment of the contract, the master copy available with the RailTel Administration shall be final and binding upon me/us.
4. I/we declare and certify that I/we have not made any misleading or false representation in the forms, statements and attachments in proof of the qualification requirements.
5. I/we also understand that my/our offer will be evaluated based on the documents/credentials submitted along with the offer and same shall be binding upon me/us.
6. I/we declare that the information and documents submitted along with the EOI by me/us are correct and I/we are fully responsible for the correctness of the information and documents, submitted by us.
7. I/we undersigned that if the certificates regarding eligibility criteria submitted by us are found to be forged/false or incorrect at any time during process for evaluation of EOI, it shall lead to forfeiture of the EOI EMD besides banning of business for five years on entire RailTel. Further, I/we (insert name of the BA)* and all my/our constituents understand that my/our constituents understand that my/our offer shall be summarily rejected.
8. I/we also understand that if the certificates submitted by us are found to be false/forged or incorrect at any time after the award of the contract, it will lead to termination of the contract, along with forfeiture of EMD/SD and Performance guarantee besides any other action provided in the contract including banning of business for five years on entire RailTel.

DEPONENT
SEAL AND SIGNATURE OF THE BA

VERIFICATION

I/We above named EOI do hereby solemnly affirm and verify that the contents of my/our above affidavit are true and correct. Nothing has been concealed and no part of it is false.

DEPONENT

SEAL AND SIGNAURE OF THE ADVOCATE

Place:
Dated:

**The contents in Italics are only for guidance purpose. Details as appropriate are to be filled in suitably by BA. Attestation before Magistrate/ Notary Public.

Annexure 5: Draft Non-Disclosure Agreement

(To be submitted on a Rs. 500 Stamp Paper)

This Non-Disclosure Agreement ("Non-Disc") is made and entered into_____day of _____ month_____year (effective date) by and between _____ ("Department") and _____("Company"). Whereas, Department and Company have entered into an Agreement ("Agreement") _____ effective_____for_____and

Whereas, each party desires to disclose to the other party certain information in oral or written form which is proprietary and confidential to the disclosing party, ("CONFIDENTIAL INFORMATION").

NOW, THEREFORE, in consideration of the foregoing and the covenants and agreements contained herein, the parties agree as follows:

1. **Definitions. As used herein:**
    a. The term "Confidential Information" shall include, without limitation, all information and materials, furnished by either Party to the other in connection with citizen/users/persons/customers data, products and/or services, including information transmitted in writing, orally, visually, (e.g. video terminal display) or on magnetic or optical media, and including all proprietary information, customer and prospect lists, trade secrets, trade names or proposed trade names, methods and procedures of operation, commercial or marketing plans, licensed document know-how, ideas, concepts, designs, drawings, flow charts, diagrams, quality manuals, checklists, guidelines, processes, formulae, source code materials, specifications, programs, software packages, codes and other intellectual property relating to the disclosing party's data, computer database, products and/or services. Results of any tests, sample surveys, analytics, data mining exercises or usages etc. carried out by the receiving party in connection with the Department's information including citizen/users/persons/customers personal or sensitive personal information as defined under any law for the time being in force shall also be considered Confidential Information.
    b. The term, "Department" shall include the officers, employees, agents, consultants, contractors and representatives of Department.
    c. The term, "Company" shall include the directors, officers, employees, agents, consultants, contractors and representatives of Company, including its applicable affiliates and subsidiary companies.
2. **Protection of Confidential Information:** With respect to any Confidential Information disclosed to it or to which it has access, Company affirms that it shall:
    a. Use the Confidential Information as necessary only in connection with Project and in accordance with the terms and conditions contained herein;

b. Maintain the Confidential Information in strict confidence and take all reasonable steps to enforce the confidentiality obligations imposed hereunder, but in no event take less care with the Confidential Information that the parties take to protect the confidentiality of its own proprietary and confidential information and that of its clients;
c. Not to make or retain copy of any commercial or marketing plans, citizen/users/persons/customers database, Bids developed by or originating from Department or any of the prospective clients of Department except as necessary, under prior written intimation from Department, in connection with the Project, and ensure that any such copy is immediately returned to Department even without express demand from Department to do so;
d. Not disclose or in any way assist or permit the disclosure of any Confidential Information to any other person or entity without the express written consent of the other party; and
e. Return to the other party, or destroy, at Department's discretion, any and all Confidential Information disclosed in a printed form or other permanent record, or in any other tangible form (including without limitation, all copies, notes, extracts, analyses, studies, summaries, records and reproductions thereof) immediately upon the earlier to occur of (i) expiration or termination of either party's engagement in the Project, or
(ii) the request of the other party therefore.
f. Not to discuss with any member of public, media, press, any or any other person about the nature of arrangement entered between Department and Company or the nature of services to be provided by the Company to the Department.

3. **Onus.** Company shall have the burden of proving that any disclosure or use inconsistent with the terms and conditions hereof falls within any of the foregoing exceptions.
4. **Exceptions.** These restrictions as enumerated in section 1 of this Agreement shall not apply to any Confidential Information:
    a. Which is independently developed by Company or lawfully received from another source free of restriction and without breach of this Agreement; or
    b. After it has become generally available to the public without breach of this Agreement by Company; or
    c. Which at the time of disclosure to Company was known to such party free of restriction and evidenced by documentation in such party's possession; or
    d. Which Department agrees in writing is free of such restrictions.
    e. Which is received from a third party not subject to the obligation of confidentiality with respect to such Information;
5. **Remedies.** Company acknowledges that

(a) any actual or threatened disclosure or use of the Confidential Information by Company would be a breach of this agreement and may cause immediate and irreparable harm to Department;

(b) Company affirms that damages from such disclosure or use by it may be impossible to measure accurately; and

(c) injury sustained by Department may be impossible to calculate and remedy fully. Therefore, Company acknowledges that in the event of such a breach, Department shall be entitled to specific performance by Company of Company's obligations contained in this Agreement. In addition, Company shall indemnify Department of the actual and liquidated damages which may be demanded by Department. Moreover, Department shall be entitled to recover all costs (including reasonable attorneys' fees) which it or they may incur in connection with defending its interests and enforcement of legal rights arising due to a breach of this agreement by Company.

6. **Need to Know.** Company shall restrict disclosure of such Confidential Information to its employees and/or consultants with a need to know (and advise such employees of the obligations assumed herein), shall use the Confidential Information only for the purposes set forth in the Agreement, and shall not disclose such Confidential Information to any affiliates, subsidiaries, associates and/or third party without prior written approval of the disclosing party.
7. **Intellectual Property Rights Protection.** No license to a party, under any trademark, patent, copyright, design right, mask work protection right, or any other intellectual property right is either granted or implied by the conveying of Confidential Information to such party.
8. **No Conflict.** The parties represent and warrant that the performance of its obligations hereunder does not and shall not conflict with any other agreement or obligation of the respective parties to which they are a party or by which the respective parties are bound.
9. **Authority.** The parties represent and warrant that they have all necessary authority and power to enter into this Agreement and perform their obligations hereunder.
10. **Dispute Resolution.** If any difference or dispute arises between the Department and the Company in connection with the validity, interpretation, implementation or alleged breach of any provision of this Agreement, any such dispute shall be referred appropriately to RailTel/ stakeholders/ partners/ patrons.
    a. The arbitration proceedings shall be conducted in accordance with the (Indian) Arbitration and Conciliation Act, 1996 and amendments thereof.
    b. The place of arbitration shall be Mumbai.
    c. The arbitrator's award shall be substantiated in writing and binding on the parties.
    d. The proceedings of arbitration shall be conducted in English language.
    e. The arbitration proceedings shall be completed within a period of 180 days from the date of reference of the dispute to arbitration.
11. **Governing Law.** This Agreement shall be interpreted in accordance with and governed by the substantive and procedural laws of India and the parties hereby consent to the exclusive

jurisdiction of Courts and/or Forums situated at Mumbai, India only.

12. **Entire Agreement.** This Agreement constitutes the entire understanding and agreement of the parties, and supersedes all previous or contemporaneous agreement or communications, both oral and written, representations and under standings among the parties with respect to the subject matter hereof.
13. **Amendments.** No amendment, modification and/or discharge of this Agreement shall be valid or binding on the parties unless made in writing and signed on behalf of each of the parties by their respective duly authorized officers or representatives.
14. **Binding Agreement.** This Agreement shall be binding upon and inure to the benefit of the parties hereto and their respective successors and permitted assigns.
15. **Severability.** It is the intent of the parties that in case any one or more of the provisions contained in this Agreement shall be held to be invalid or unenforceable in any respect, such provision shall be modified to the extent necessary to render it, as modified, valid and enforceable under applicable laws, and such invalidity or unenforceability shall not affect the other provisions of this Agreement.
16. **Waiver.** If either party should waive any breach of any provision of this Agreement, it shall not thereby be deemed to have waived any preceding or succeeding breach of the same or any other provision hereof.
17. **Survival.** Both parties agree that all of their obligations undertaken herein with respect to Confidential Information received pursuant to this Agreement shall survive till perpetuity even after any expiration or termination of this Agreement.
18. **Non-solicitation.** During the term of this Agreement and thereafter for a further period of two (2) years Company shall not solicit or attempt to solicit Department's employees and/or consultants, for the purpose of hiring/contract or to proceed to conduct operations/business similar to Department with any employee and/or consultant of the Department who has knowledge of the Confidential Information, without the prior written consent of Department. This section will survive irrespective of the fact whether there exists a commercial relationship between Company and Department.
19. **Term.** Subject to aforesaid section 17, this Agreement shall remain valid up to __years from the "effective date".

IN WITNESS HEREOF, and intending to be legally bound, the parties have executed this Agreement to make it effective from the date and year first written above.

For Department

Name:

Title:

WITNESSES:

1. _____

_____

2. _____

_____

For Company

Name:

Title:

WITNESSES:

1. _____

_____

2. _____

_____

Annexure 6: Integrity Pact

(To be executed on Rs. 500/- Stamp Paper)

EoI Number:_____Dated: _____

This Integrity Pact is made at on this _____Day of_____2024

BETWEEN

RailTel Corporation of India Ltd (a Govt of India Enterprise under Ministry of Railways) having its registered office at Plate-A, 6th Floor, Office Block Tower-2, East Kidwai Nagar, New Delhi-110023and Regional Office at Western Railway Microwave Complex, Senapati Bapat Marg, Mahalaxmi, Mumbai – 400013, hereinafter referred to as "The Principal", which expression shall unless repugnant to the meaning or contract thereof include its successors and permitted assigns
AND
<Bidder Name> having its registered office at <Bidders Registered and Branch Address (if any)> hereinafter referred to as "The Bidder/ Contractor/ Concessionaire/ Consultant" and which expression shall unless repugnant to be meaning or context thereof include its successors and permitted assigns.

Preamble

Whereas, the principal intends to award, under laid down organizational procedures contract/s for 'Implementation of unified communication infrastructure comprising IPMPLS LAN infra, VOIP exchange, IP based control communication and replacement of UTN over Western Railways.' The Principal values full compliance with all relevant laws of the land, rules of land, regulations, economic use of resources and of fairness/ transparency in its relations with its Bidder(s) and for Contractor(s)/Concessionaire(s)/Consultant(s).

And whereas to meet the purpose aforesaid, both the parties have agreed to enter into this Integrity Pact (hereafter referred to as Integrity Pact) the terms and conditions of which shall also be read as integral part and parcel of the Tender documents and contract between the parties. Now, therefore, in consideration of mutual covenants stipulated in this pact, the parties hereby agree as follows and this pact witnesseth as under: -

Article – 1: Commitments of the Principal

1. The principal commits itself to take all measures necessary to prevent corruption and to observe the following principles: -

a. No employee of the Principal, personally or through family members, will in connection with the Tender for, or the execution of a contract, demand take a promise for or accept for self or third person any material or immaterial benefit which the person is not legally entitled to.
b. The principal will, during the tender process treat all Bidder(s) with equity and reason. The principal will in particular, before and during the tender process, provide to all Bidder(s) the same information and will not provide to any Bidder(s) confidential/ additional information through which the Bidder(s) could obtain an advantage in relation to the tender process or the contract execution.
c. The principal will exclude all known prejudiced persons from the process.

2. If the Principal obtains information on the conduct of any of its employees which is a criminal offence under the IPC/PC Act or any other Statutory Acts or if there be a substantive suspicion in this regard, the principal will inform the Chief Vigilance Officer and in addition can initiate disciplinary actions as per its internal laid down Rules/ Regulations.

Article – 2: Commitments of the Bidder(s)/ Contractor(s)/ Concessionaire(s)/ Consultant(s)

The Bidder(s)/ Contractor(s)/ Concessionaire(s)/ Consultant(s) commit himself to take all measures necessary to prevent corruption. He commits himself to observe the following principles during his participation in the tender process and during the contract execution.

a. The Bidder(s)/ Contractor(s)/ Concessionaire(s)/ Consultant(s) will not, directly or through any other person or firm, offer, promise or give to any of the Principals employees involved in the tender process or the execution of the contract or to any third person any material or other benefit which he/she is not legally entitled to, in order to obtain in exchange any advantage of any kind whatsoever during the tender process or during the execution of the contract.
b. The Bidder(s)/ Contractor(s)/ Concessionaire(s)/ Consultant(s) will not enter with other Bidders into any undisclosed agreement or understanding, whether formal or informal. This applies in particular to prices, specifications, certifications, subsidiary contracts, submission or non-submission or bids or any other actions to restrict competitiveness or to introduce cartelization in the bidding process.
c. The Bidder(s)/ Contractor(s)/ Concessionaire(s)/ Consultant(s) will not commit any offence under the relevant IPC / PC. Act and other Statutory Acts; further the Bidder(s)/ Contractor(s)/ Concessionaire(s)/ Consultant(s) will not use improperly for purposes of completion or personal gain, or pass on to others, any information or document provided by the Principal as part of the business relationship, regarding plans, technical proposals and business details, including information contained or transmitted electronically.

d. The Bidder(s)/ Contractor(s)/ Concessionaire(s)/ Consultant(s) of foreign origin shall disclose the name and address of the Agents/ representatives in India. If any similarly the Bidder(s)/ Contractor(s)/ Concessionaire(s)/ Consultant(s) of Indian Nationality shall furnish the name and address of the foreign principle, if any. Further details as mentioned in the 'Guidelines on Indian Agents of Foreign Suppliers' shall be disclosed by the Bidder(s)/ Contractor(s)/ Concessionaire(s)/ Consultant(s). Further, all the payments made to the Indian Agent /Representative have to be Indian Rupees only.
e. The Bidder(s)/ Contractor(s)/ Concessionaire(s)/ Consultant(s) will, when presenting his bid, disclose any and all payments he has made, is committed to or intends to make to agents, brokers or any other intermediaries in connection with the award of the contract. He shall also disclose the details of services agreed upon for such payments.
f. The Bidder(s)/ Contractor(s)/ Concessionaire(s)/ Consultant(s) will not instigate third persons to commit offences outlined above or be an accessory to such offences.
g. The Bidder(s)/ Contractor(s)/ Concessionaire(s)/ Consultant(s) will not bring any outside influence through any Govt. bodies/quarters directly or indirectly on the bidding process in furtherance of his bid.
h. The Bidder(s)/ Contractor(s)/ Concessionaire(s)/ Consultant(s) who have signed an Integrity pact shall not approach the court while representing the matter to IEMs and shall wait for their decision in the matter.

Article – 3: Disqualification from tender process and exclusion from future contracts

1. If the Bidder(s)/ Contractor(s)/ Concessionaire(s)/ Consultant(s) before award or during execution has committed a transgression through a violation of any provision of Article-2, above or in any other form such as to put his reliability or credibility in question, the Principal is entitled to disqualify the Bidder(s)/ Contractor(s)/ Concessionaire(s)/ Consultant(s) from the tender process.
2. If the Bidder/Contractor/Concessionaire/Consultant has committed a transgression through a violation of Article-2 such as to put his reliability or credibility into question, the principal shall be entitled to exclude including blacklist and put on holiday the Bidder/Contractor/ Concessionaire/ Consultant for any future tenders/contract award process. The imposition and duration of the exclusion will be determined by the severity of the transgression. The severity will be determined by the principal taking into consideration the full facts and circumstances of each case particularly taking into account the number of transgressions, the position of the transgressors within the company hierarchy of the Bidder/Contractor/Concessionaire/Consultant and the amount of the damage. The exclusion will be imposed for a maximum of 1 year.

3. A transgression is considered to have occurred if the principal after due consideration of the available evidence concludes that "On the basis of facts available there are no material doubts".
4. The Bidder/ Contractor/Concessionaire/Consultant will its free consent and without any influence agrees and undertakes to respect and uphold the principal's absolute rights to resort to and impose such exclusion and further accepts and undertakes not to challenge or question such exclusion on any ground, including the lack of any hearing before the decision to resort to such exclusion is taken. This undertaking is given freely and after obtaining independent legal advice.
5. The decision of the principal to the effect that a breach of the provisions of this Integrity Pact has been committed by the Bidder/ Contractor/Concessionaire/Consultant shall be final and binding on the Bidder/ Contractor/Concessionaire/Consultant, however, the Bidder/ Contractor/ Concessionaire/ Consultant can approach IEM(s) appointed for the purpose of this Pact.
6. On occurrence of any sanctions/ disqualification etc. arising out from violation of integrity pact, Bidder/ Contractor/Concessionaire/Consultant shall not be entitled for any compensation on this account.
7. Subject to full satisfaction of the principal, the exclusion of the Bidder/Contractor/Concessionaire/Consultant could be revoked by the principal if the Bidder/ Contractor/Concessionaire/Consultant can prove that he has restored/recouped the damage caused by him and has installed a suitable corruption prevention system in his organization.

Article – 4: Compensation for Damages

1. If the Principal has disqualified the Bidder(s) from the tender process prior to the award according to Arcticle-3, the principal shall be entitled to forfeit the Earnest Money Deposit/ Bid Security or demand and recover the damages equivalent to Earnest Money Deposit/ Bid Security apart from any other legal right that may have accrued to the principal.
2. In addition to the above, the principal shall be entitled to take recourse to the relevant provisions of the contract related to Termination of Contract due to Contractor/Concessionaire/Consultant's Default. In such case, the principal shall be entitled to forfeit the Performance Bank Guarantee of the Contractor/ Concessionaire/ Consultant and/or demand and recover liquidated and all damages as per the provisions of the contact/Concession agreement against Termination.

Article – 5: Previous Transgression

1. The Bidder declares that no previous transgression occurred in the last 3 years immediately before signing of this integrity pact with any other Company in any country conforming to the anticorruption/Transparency International (TI) approach or with any

other Public Sector Enterprise/Undertaking in India or any Government Department in India that could justify his exclusion from the Tender process.

2. If the Bidder makes incorrect statement on this subject, he can be disqualified from the tender process or action for his exclusion can be taken as mentioned under Article-3 above for transgression of Article-2 and shall be liable for compensation for damages as per Article-4 above.

Article – 6: Equal treatment of all Bidders/ Contractors/ Concessionaires/ Consultants/ Subcontractors

1. The Bidder(s)/Contractor(s)/Concessionaire(s)/Consultant(s) undertake(s) to demand from all sub-contractors a commitment in conformity with this integrity Pact, and to submit it to the principal before contract signing.
2. The principal will enter into agreements with identical conditions as this one with all Bidders/Contractors/Concessionaire/Consultant and Subcontractors.
3. The principal will disqualify from the Tender process all Bidders who do not sign this Pact violate its provisions.

Article – 7: Criminal charges against violating Bidder(s)/ Contractor(s)/ Concessionaire(s)/ Consultant(s)/ Sub-contractor(s)

If the Principal obtains knowledge of conduct of a Bidder/ Contractor/ Concessionaire/ Consultant or Subcontractor, or of an employee or a representative or an associate of a Bidder/ Contractor/ Concessionaire/ Consultant or Subcontractor, which constitutes corruption, or if the principal has substantive suspicion in this regard, the principal will inform the same to the Chief Vigilance Officer.

Article – 8: Independent External Monitor (IEM)

1. The principal appoints competent and credible Independent External Monitor for this Pact after approval from the Central Vigilance Commission. The task of the Monitor is to review independently and objectively, whether and to what extent the parties comply with the obligations under this agreement.
2. The Monitor is not subject to instructions by the representatives of the parties and performs his functions neutrally and independently. He reports to the CMD, RailTel.
3. The Bidder/Contractor/Concessionaire/Consultant accepts that the Monitor has the right to access without restriction to all Project documentation of the principal including that provided by the Bidder/ Contractor/ Concessionaire/ Consultant. The Bidder/ Contractor/ Concessionaire/ Consultant will also grant the Monitor, upon his request and demonstration of valid interest, unrestricted and unconditional access to his Project documentation. The same is applicable to Subcontractors.
4. The Monitor is under contractual obligation to treat the information and documents of the Bidder(s)/Contractor(s)/Subcontractors(s) with confidentiality. The Monitor has also

signed on ‘Non-disclosure of Confidential Information’ and of ‘Absence of Conflict of Interest’. In case of any conflict of interest arising at a later date, the IEM shall inform CMD, RailTel and recuse himself/herself from that case.

5. The principal will provide to the Monitor sufficient information about all meetings among the parties related to the Project provided such meetings could have an impact on the contractual relations between the Principal and the Bidder/Contractor/ Concessionaire/Consultant. The parties offer to the Monitor the option to participate in such meetings.
6. As soon as the Monitor notices, or believes to notice any transgression as given in Article- 2, he may request the Management of the Principal to take corrective action, or to take relevant action. The monitor can in this regard submit non-*binding recommendations. Beyond this, the Monitor has no right to demand from the parties that they act in a specific manner, refrain from action or tolerate action.
7. The Monitor will submit a written report to the CMD, RailTel within 8-10 weeks from the date of reference or intimation to him by the principal and, should the occasion arise, submit proposals for correcting problematic situations.
8. If the Monitor has reported to the CMD, RailTel, a substantiated suspicion of an offence under relevant IPC/PC Act or any other Statutory Acts, and the CMD, RailTel has not, within the reasonable time taken visible action to proceed against such offence or reported it the Chief Vigilance Officer, the Monitor may also transmit this information directly to the Central Vigilance Commissioner.
9. The word 'Monitor' would include both singular and plural.

Article – 9: Pact Duration

This Pact begins when both parties have legally signed it. It expires for the Contractor/Consultant 12 months after his Defect Liability Period is over or 12 months after his last payment under the contract whichever is later and for all other unsuccessful Bidders, 6 months after this Contract has been awarded (In case of BOT projects). It expires for the concessionaire 24 months after his concession period is over and for all other unsuccessful Bidders 6 months after this Contract has been awarded. Any violation of the same would entail the disqualification of the bidder and exclusion from future dealings.

If any claim is made/lodged during this time, the same shall be binding and continue to be valid despite the lapse of this pact as specified above, unless it is discharged determined by CMD of RailTel.

Article – 10: Other Provisions

1. This pact is subject to Indian Law, Place of performance and jurisdiction is the Registered Office of the Principal, i.e. New Delhi.
2. Changes and supplements as well as termination notices need to be made in writing.
3. If the Bidder/Contractor/Concessionaire/Consultant is a partnership or a Joint Venture partner, this pact must be signed by all partners or members.
4. Should one or several provisions of this agreement turn out to be invalid, the reminder of this agreement remains valid, in this case, the parties will strive to come to an agreement to their original intentions.
5. Issue like warranty / Guarantee etc. shall be outside the purview of IEMs.
6. In the event of any contradiction between the Integrity Pact and its Annexure, the clause in Integrity Pact shall prevail.
7. Any dispute/differences arising between the parties with regard to term of this Pact, any action taken by the principal in accordance with this Pact or interpretation thereof shall not be subject to any Arbitration.
8. The actions stipulated in the integrity Pact are without prejudice to any other legal action that may follow in accordance with the provisions of the extant law in force relating to any civil or criminal proceedings.

In witness whereof he parties have signed and executed this pact at the place and date first mentioned in the presence of following witnesses: -

(For & On behalf of the (Principal)

(For & On behalf of Bidder/Contractor/ Concessionaire/Consultant)

Place:
Date:

Witness 1:

_____

Witness 2:

Annexure 7: Complete EoI Examination & Nil Deviation Certificate

(To be submitted by Bidder)

To
Deputy General Manager/ Marketing
RailTel Corporation of India Ltd
Western Railway Microwave Complex
Senapati Bapat Marg, Near Railway Sports Ground
Mahalaxmi, Mumbai – 400013

Sub: Complete EoI Examination & Nil Deviation Certificate

Ref: EoI Number:_____Dated: _____

Dear Sir,

We <Bidder Name> having completely examined the referred EoI, its corrigendum and any other documents/its addendums/corrigendum referred in this EoI, conclude that we have understood the Terms & Conditions of the EoI and its subsequent addendums & corrigendum (if any) and any other documents/its addendums/corrigendum referred in this EoI. We declare that we have sought all clarifications for the same from RailTel or its end customer for anything contained in this EoI & any other documents/its addendums/ corrigendum referred in this EoI and have been satisfied with the clarifications to the fullest extent and there are no terms, clauses, conditions, etc which are ambiguous.

We also declare that there is no deviation from adhering to anything that is contained in this EoI and any other documents/its addendums/corrigendum referred in this EoI and that any deviation later raised by us shall lead to forfeiture of the Bid/Contract at complete discretion of RailTel.

Signature of Authorized Signatory (with official seal)
Name :
Designation :
Address :
Telephone and Fax :
E-mail address :

Annexure 8: Back-to-Back Compliance Certificate

(To be submitted by Bidder)

To
Deputy General Manager/ Marketing
RailTel Corporation of India Ltd
Western Railway Microwave Complex
Senapati Bapat Marg, Near Railway Sports Ground
Mahalaxmi, Mumbai – 400013

Sub: Complete back-to-back Compliance Certificate

Ref: 1) EoI Number:_____Dated: _____
2) Bid No: GEM/2025/B/6200863 dated 19th May, 2025 and all of its addendums/ corrigendum's & published documents.

Dear Sir,

Considering reference 1 & 2 we would like to declare that we have read and understood the EoI, its corrigendum and any other documents/its addendums/corrigendum referred in this EoI thoroughly. We would like to give you our back-to-back compliance for all the tender terms and conditions, clauses, timelines, deliverables and anything explicitly mentioned in the EoI, its corrigendum and any other documents/its addendums/corrigendum referred in this EoI.

Signature of Authorized Signatory (with official seal)
Name :
Designation :
Address :
Telephone and Fax :
E-mail address :

Annexure 9: Performance Bank Guarantee Format

(For a sum of x% of the value of the contract as per RailTel's end customer RFP/tender)
(Stamp Duty to be confirmed by RailTel in co-ordination with RailTel's Legal Department)

Ref. No. :
Date :
Bank Guarantee No. :

To
<Insert complete postal address>

THIS INDENTURE made this <current date> day of <current Month> 2024, BETWEEN THE <Bank Name>, a Company incorporated and registered under the Indian companies act, 1913 and deemed to exist within the companies Act 1956, and governed by the Banking Regulation Act, 1949 and having its registered office at <Address>, and its corporate office at <Address>, India and having one of its Branch Office at <Mumbai Branch Office> (hereinafter referred to as "the Bank" which expression shall be deemed to includes its successors and assigns) of the first part and

<Bidders Company Name> a company incorporated under the Indian Companies Act 1956 having its Registered Office at <Address>, Corporate Office at <Address> and its Regional Office at <Mumbai Office Address> (hereinafter referred to as 'the Contractor/s') of the second part and

RailTel Corporation of India Ltd (hereinafter referred to as 'RailTel') of the third part WHEREAS the Contractor/s have submitted to RailTel EoI/Quotation for the execution of Implementation of unified communication infrastructure comprising IPMPLS LAN infra, VOIP exchange, IP based control communication and replacement of UTN over Western Railways vide <EoI No> Dated <Date of EoI> and the terms of such EoI/Tender/Quotation/contract require that the Contractor/s shall deposit with RailTel as the security a sum of Rs. <Amount>/- (in figures and words<in words> only Including all Taxes and contingencies and any other costs mentioned as per LOI and RailTel Terms)AND WHEREAS if and when any such EoI/Tender/Quotation is accepted by RailTel the contract to be entered into in furtherance thereof by the Contractor/s will provide that such deposit shall remain with and be appropriated by RailTel towards the security deposit to be taken under the contract and be redeemable by the Contractors/ if they shall duly and faithfully carry out the terms and provision of such contract and shall duly satisfy all claims properly chargeable against them there under AND WHEREAS the Contractor/s are constituents of the Bank and in order to facilitate the keeping of the accounts of the Contractor/s, the Bank with the consent and concurrence of the Contractor/s has requested RailTel to accept the Guarantee of the Bank hereinafter contained, in place of the Contractor/s

depositing with RailTel the said sum as security as aforesaid AND WHERE AS accordingly <Bank Name>has agreed to accept claim from RailTel upon demand in writing, whenever required by him, from time to time upto <Date (contract period + 3 months)> so to do, a sum not exceeding in the whole Rs. <Amount>/- (in figures and words <in words> only incl of Tax) under the terms of the said EoI/Tender/Quotation and/ or the Contract. The Bank Guarantee is valid up to<Date (contract period + 3 months)>.

Notwithstanding anything what has been stated above, <Bank Name> liability under the above guarantee is restricted to Rs. <Amount>/- (in figures and words <in words>only incl of Tax) and guarantee shall remain in force up to <Date (contract period + 3 months)> unless the demand or claim under this guarantee is made on us and we receive in writing on or before <Date (contract period + 3 months)> all your rights under the above guarantee shall be forfeited and we shall be released from all liabilities under the guarantee thereafter whether or not the original bank guarantee is returned to us.

In witness whereof the Bank, through its authorized Officer, has set its hand and stamp on this …… day of 2025 at ……

For <Bank Name>

Authorized Signatories

EMP No._____

For<Company Name>

Authorized Signatories

EMP No._____

Annexure 10: BoQ

NUMBER #	TEXT #	NUMBER #	TEXT #	TEXT #	NUMBER #	NUMBER #	TEXT #
Sl. No.	Item Description	Quantity	Units	Quoted Currency in INR / Other Currency	BASIC RATE In Figures To be entered by the Bidder Without GST Rs.	TOTAL AMOUNT Without GST	TOTAL AMOUNT In Words
1	2	4	5	12	13	53	55
1	**Provisioning of Cloud Service provider for BMC**						
1.01	Existing Cloud Workload	36	Nos	INR		0.00	INR Zero Only
1.02	LINUX virtual machine (RHEL latest version with Enterprise License support included for the OS) Specification: 4vCPU/8GB RAM/100 GB SSD / 1:2 vCPU/VM (VMs require DC + Cold DR)	792	Nos	INR		0.00	INR Zero Only
1.03	Enterprise License support included for the OS) Specification: 4vCPU/8GB RAM/100 GB SSD / 1:2 vCPU/VM (VMs require DC + Cold DR)	72	Nos	INR		0.00	INR Zero Only
1.04	LINUX virtual machine (RHEL latest version with Enterprise License support included for the OS) Specification: 16vCPU/32GB RAM/100 GB SSD / 1:2 vCPU/VM/16 GB GPU (VMs require DC + Cold DR)	36	Nos	INR		0.00	INR Zero Only
1.05	Windows virtual machine (Enterprise grade Latest Windows with Enterprise License support included for the OS) Specification: 16vCPU/32GB RAM/100 GB SSD / 1:2 vCPU/VM/16 GB GPU (VMs require DC + Cold DR)	36	Nos	INR		0.00	INR Zero Only
1.06	LINUX virtual machine (Ubantu/RHEL latest version with Enterprise License support included for the OS) Specification: 8vAPU/32GB RAM/250 GB SSD (VMs require DC + Cold DR)	252	Nos	INR		0.00	INR Zero Only
1.07	Windows virtual machine (Enterprise grade Latest Windows with Enterprise License support included for the OS) Specification: 8vAPU/32GB RAM/250 GB SSD (VMs require DC + Cold DR)	180	mtr	INR		0.00	INR Zero Only
1.08	Additional CPU	8820	Nos	INR		0.00	INR Zero Only
1.09	Additional Memory	54000	Nos	INR		0.00	INR Zero Only
1.1	DR Agent (Cloud DC to Cloud DR)	2160	Nos	INR		0.00	INR Zero Only
1.11	Additional Block Storage to be attached to VM - SSD High IOPS (5000 IOPS and 200 MB/s throughput per TB) (DC+DR)	4500	Nos	INR		0.00	INR Zero Only
1.12	File Share Storage (EFS/NAS) - between multiple virtual machines - SSD	1872	Nos	INR		0.00	INR Zero Only
1.13	Backup Agent	2160	Nos	INR		0.00	INR Zero Only
1.14	Backup Storage	7560	Nos	INR		0.00	INR Zero Only
1.15	Internet Link (500Mbps)	36	Nos	INR		0.00	INR Zero Only
1.16	Data Replication (Cloud DC-Cloud DR) 12000 GB/Month	36	Nos	INR		0.00	INR Zero Only
1.17	SD-WAN link(Solution with necessary licenses and hardware (if any)	1	Nos	INR		0.00	INR Zero Only
1.18	SD-WAN/P2Plink(DC) (primary+secondary) (2 location(CSP to WDC) (Requirement - 500mbps) per link/year	6	Nos	INR		0.00	INR Zero Only
1.19	SD-WAN/ P2P Link (DR) (3 location(DR to WDC) (Requirement - 150 Mbps) per link/year	3	Nos	INR		0.00	INR Zero Only
1.2	Load Balancer as a service (5 rules)	540	Nos	INR		0.00	INR Zero Only
1.21	Public IP Address	1080	Nos	INR		0.00	INR Zero Only
1.22	Firewall as a Service (UTM/IPS/IDS)	36	Nos	INR		0.00	INR Zero Only
1.23	Web Application Firewall (vWAF/cWAF) with 10 rules	36	Nos	INR		0.00	INR Zero Only
1.24	DDOS Protection	1	Nos	INR		0.00	INR Zero Only
1.25	VMDR (Vulnerability Management, Detection, and Response)	1	Nos	INR		0.00	INR Zero Only
1.26	WAS (Web Application Scanning)WAS (Web Application Scanning)	1	Nos	INR		0.00	INR Zero Only
1.27	Threat Vision	1	Nos	INR		0.00	INR Zero Only
1.28	CSPM (Cloud Security Posture Management)	1	Nos	INR		0.00	INR Zero Only
1.29	Microsegmentation Security	1	Nos	INR		0.00	INR Zero Only
1.3	Wild card SSL Certificate (support unlimited sub- domains)	3	Nos	INR		0.00	INR Zero Only
1.31	P2P Cross Connect /Termination Charges (DC)	72	Nos	INR		0.00	INR Zero Only
1.32	P2P Cross Connect /Termination Charges (DR)	36	Nos	INR		0.00	INR Zero Only
1.33	One Time Implementation and Migration Charge	1	lumpsum	INR		0.00	INR Zero Only
1.34	Migration Charges for 3D GIS	1	lumpsum	INR		0.00	INR Zero Only
1.35	MSP Charges	36	lumpsum	INR		0.00	INR Zero Only
Total in Figures						0.00	INR Zero Only
Quoted Rate in Words						**INR Zero Only**	

Brihanmumbai Municipal Corporation

Information Technology Department

Request for Bids

RFB No: 2025_MCGM_1182423_1 dated29.05.2025

Provisioning, Configuration, Testing, Commissioning, Operations & Maintenance of Cloud Services for BMC

Brihanmumbai Municipal Corporation
(Information Technology Department)

No. Director/IT/550827 Dated 28/05/2025.

Notice Inviting Tender (NIT)

1. The Commissioner of Brihanmumbai Municipal Corporation invites e-bids for the work mentioned below. The bid copy can be downloaded from Mahatendersportal (https://mahatenders.gov.in/nicgep/app) -> "Tenders by Organization" tab -> Municipal Corporation of Greater Mumbai.
2. All interested Bidders, whether already registered or not registered in BMC, are mandated to get registered with Mahatenders for e-Tendering process and obtain Login Credentials to participate in the Online bidding process. The details of the same are available on the above-mentioned Mahatenders portal under 'Help for Contractors'.
3. The Bidders can get digital signatures from any one of the certifying Authorities (CA's) licensed by the Controller of Certifying Authorities published under Licensed CAs. A list of CAs is available on https://cca.gov.in/licensed_ca.html
4. The technical and commercial bids shall be submitted online up to the end date & time mentioned below.

#	Description	Tender Fee	Bid Security (EMD)	Start date &Time for online Bid Downloading	End date &Time for online Bid Submission
1	Provisioning, Configuration, Testing, Commissioning, Operations & Maintenance of Cloud Services For BMC Bid No. 2025_MCGM_1182423_1	Rs.30250/- + 18% GST Total Rs. 35695/-	Rs. 1,16,89,351/-	29.05.2025 at 11.00 hrs	18.06.2025 at 16.00 hrs
Note: Last date for online payment of Bid Security / Earnest money Deposit (EMD) is before due / end date & time for online Bid Submission prescribed above.					

5. The pre-bid meeting will be held on **04.06.2025 at 15.00 hours**, at venue – Office of Director (IT), Basement, Annex. Building, Municipal Head Office, 1, Mahapalika Marg, Fort, Mumbai – 400 001.
6. The prospective Bidder(s) should submit their suggestions/observations, if any, by email to director.it@mcgm.gov.inwith a copy to am01.it@mcgm.gov.inbefore 2 days of Pre-bid meeting. Only suggestions / observations received by email will be discussed and clarified in pre-bid meeting and any modification of the bidding documents, which may become necessary as a result of pre-bid meeting, shall be made by BMC exclusively through the issue of an addendum/corrigendum and shall be published on https://mahatenders.gov.in/nicgep/app
7. Bidders shall note that any corrigendum issued regarding this E-Procurement notice will be published on the https://mahatenders.gov.in/nicgep/app portal only. No corrigendum will be published in the local newspapers.
8. The Bid document uploaded shall be read in conjunction with any addendum / corrigendum. A maximum of two authorized representatives of prospective Bidder(s), who have an authorization letter to attend the pre-bid meeting, can attend the pre-bid meeting and obtain clarification regarding specifications, works & Bid conditions.

9. The Bidder shall have to pay "Tender Fee" through online payment only.
10. The Bidder shall have to pay Bid Security / Earnest Money Deposit (EMD) through online payment only. Note: - No Exemption will be allowed for the Bidders having a standing deposit with BMC.
11. Bidders are advised to complete the online payment (if applicable) for Tender Fee/ EMD and other fees well in advance at least one day in advance prior to the bid submission due date/time to avoid the last-minute hassles.
12. Bidders who are using SB MOPS other banks Internet Banking are requested to make online payment four days in advance.
13. For online Payment related issues, kindly send email with Bank Reference Number to this email ID merchant@sbi.co.in. You may also contact 022-27560149 for clarifications.
14. Bidder agencies are advised to study this bid document carefully before submitting their bids in response to the Bid Notice. Submission of a bid in response to this notice shall be deemed to have been made after careful study and examination of this document with full understanding of its terms, conditions and implications.
15. This bid document is non-transferable.
16. A three-envelope (Cover1 - Fee, Cover2 – Prequal/Technical and Cover3 - Finance) selection procedure shall be adopted.
17. Bidder (authorized signatory) shall submit their offer online in electronic formats of technical (including prequalification documents) and financial proposal.
18. BMC will not be responsible for delays in online submission due to any reason. For this, bidders are advised to upload the complete bid proposal well in advance before the due date and time so as to avoid issues like slow speed, choking of web site due to heavy load or any other unforeseen problems.
19. Bidders are also advised to refer to “Bidders Manual Kit” and Help for Contractors available at https://mahatenders.gov.in/nicgep/app for further details about the e-tendering process.
20. For any assistance on use of e-Tendering system, kindly contact helpdesk number 0120-4001 002, 0120-4001 005, 0120-4493 395, Email: support-eproc(at)nic(dot)in
21. The Authority (BMC) shall not be liable for any omission, mistake or error in respect of any of the above or on account of any matter or thing arising out of or concerning or relating to the Bid or the Bidding Process, including any error or mistake therein or in any information or data given by the Authority.
22. The Municipal Commissioner reserves the right to reject all or any of the e-Bid(s) without assigning any reason at any stage.

Sd/-

(Head of Department)

Contents

Glossary

Sr. No.	Abbreviations and Acronyms	Expansion / Full Form / Explanation/Description	Sr. No.	Abbreviations and Acronyms	Expansion / Full Form / Explanation / Description
1	AMC	Additional Municipal Commissioner	31	ESIC	Employees' State Insurance Corporation
2	API	Application Programming Interface	32	FRS	Functional Requirement Specifications
3	BDS	Bid Data Sheet	33	GBPS	Gigabits Per Second
4	BEC	Bid Evaluation Committee	34	GCC	General Conditions of Contract
5	BI	Business Intelligence	35	GIGW	Government of India Guidelines for Websites
6	BMC	Brihanmumbai Municipal Corporation	36	GIS	Geographical Information System
7	CE	City Engineer	37	GRC	Governance, Risk & Compliance
8	CA	Current Assets	38	GST	Goods & Services Tax
9	CC (BDS Page 31)	Carbon Copy	39	HOD	Head of Department
10	CERT-In	Computer Emergency Response Team - India	40	HRM	Human Resource Management
11	CFC	Citizen Facilitation Centre	41	HTML	Hypertext Markup Language
12	CGST	Central Goods & Services Tax	42	HTTP	Hypertext Transfer Protocol
13	CL	Current Liabilities	43	HTTPS	Hypertext Transfer Protocol Secured
14	CMMi	Capability Maturity Model	44	HVAC	Heating Ventilation & Air Conditioning
15	COTS	Customizable Off-The-Shelf Software	45	ICT	Information & Communication Technology
16	CPD	Central Purchase Department	46	IDS	Intrusion Detection System
17	CPU	Central Processing Unit	47	IEEE	Institute of Electrical and Electronics Engineers
18	CRM	Customer Relationship Management	48	IIS	Internet Information Server
19	CSP	Cloud Service Provider	49	INR	Indian Rupee/s
20	CSS	Cascaded Style Sheet	50	IP	Internet Protocol
21	CSV	Comma Separated Values	51	IPR	Intellectual Property Rights
22	DBMS	Database Management System	52	IPS	Intrusion Prevention System

23	DC	Data Centre	53	IPv4	Internet Protocol Version 4
24	DMC	Deputy Municipal Commissioner	54	IPv6	Internet Protocol Version 6
25	DR	Disaster Recovery	55	IS	"Information System," means all the tools and Cloud services required to enhance IT security for BMC .
26	EDI	Electronic Data Interchange	56	ISO/IEC	International Standards Organization
27	EITM	Enterprise Information Technology Management	57	IT	Information Technology
28	EMC	Electromagnetic Compatibility	58	ITB	Instructions To Bidders
29	EMD	Earnest Money Deposit (Bid Security)	59	ITeS	Information Technology enabled Services
30	ERP	Enterprise Resource Planning	60	ITIL	Information Technology Infrastructure Library

Sr. No.	Abbreviations and Acronyms	Expansion / Full Form / Explanation/Description	Sr. No.	Abbreviations and Acronyms	Expansion / Full Form / Explanation / Description
61	JDBC	Java Database Connectivity	91	RTO	Recovery Time Objective
62	JPEG	Joint Photographic Experts Group	92	SD-WAN	Software-Defined Wide Area Network
63	JSON	Java Script Object Notation	93	SEI	Software Engineering Institute
64	JV	Joint Venture	94	SGST	State Goods & Services Tax
65	LDAP	Lightweight Directory Access Protocol	95	SIEM	Security Information & Event Management
66	LLP	Limited Liability Partnership	96	SITC	Supply, Installation, Testing & Commissioning
67	LOA	Letter of Acceptance	97	SLA	Service Level Agreement
68	LOI	Letter of Intent	98	SMS	Short Message Service
69	MBPS	Megabits Per Second	99	SOA	Service Oriented Architecture
70	MDM	Mobile Device Management	100	SOAP	Simple Object Access Protocol
71	MeitY	Ministry of Electronics & Information Technology	101	SQL	Structured Query Language
72	MMC Act 1888	Mumbai Municipal Corporation Act, 1888 (updated)	102	SSD	Solid State Drive
73	MSDG	Mobile Service Delivery Gateway	103	SSDG	State Service Delivery Gateway
74	NW	Net Worth	104	SSL	Secured Socket Layer
75	O&M	Operations &	105	STQC	Standardization Testing &

		Maintenance			Quality Certification
76	OAT	Operational Acceptance Test	106	TA	Total Assets
77	ODBC	Open Database Connectivity	107	TIFF	Tag Image File Format
78	OEM	Original Equipment Manufacturer	108	TL	Total Liabilities
79	OS	Operating System	109	TLS	Transport Layer Security
80	PAN	Permanent Account Number	110	TR	Total Revenue
81	PBT	Profits Before Tax	111	UAT	User Acceptance Test
82	PDF	Postscript Data Format	112	UI	User Interface
83	PF	Provident Fund	113	UPS	Uninterrupted Power Supply
84	QOS	Quality of Service	114	URL	Unique Resource Locator
85	RAM	Random Access Memory	115	VLAN	Virtual Local Area Network
86	RBAC	Role Based Access Control	116	VoIP	Voice Over Internet Protocol
87	RDBMS	Relational Database Management System	117	VPN	Virtual Private Network
88	RFB	Request For Bids	118	W3C	World Wide Web Consortium
89	RHEL	Red Hat Enterprise Linux	119	WAN	Wide Area Network
90	RPO	Recovery Point Objective	120	XML	Extensible Markup Language

Part I – Bidding Procedures

Section I - Instructions to Bidders

A. General

1. Scope of Bid

In connection with the Bid Notice - Request for Bids (RFB), details specified in the Bid Notice and Bid Data Sheet (BDS), BMC issues this bidding document for the delivery of Services, as specified in Section - BMC's Requirements. The name, identification, and number of this RFB procurement are specified in the BDS.

a. Throughout this bidding document:

   i. the term “in writing” means communicated in written form (e.g., by e-mail) with proof of receipt;

   ii. if the context so requires, “singular” means “plural” and vice versa; and

   iii. “Day” means calendar day, unless otherwise specified as “Business Day”. A Business Day is any day that is an official working day of BMC. It excludes the BMC’s official public holidays;

b. While every effort has been made to provide comprehensive and accurate background information and requirements and specifications, Bidders must form their own conclusions about the solution needed to meet the requirements. Bidders and recipients of this RFB may wish to consult their own legal advisers in relation to this RFB.

c. This RFB supersedes and replaces any previous public documentation & communications, and Bidders should place no reliance on such communications.

d. No commitment of any kind, contractual or otherwise shall exist unless and until a formal written contract has been executed by or on behalf of the BMC. Any notification of preferred Bidder status by the BMC shall not give rise to any enforceable rights by the Bidder. BMC may cancel this public procurement at any time prior to a formal written contract being executed by or on behalf of the BMC.

2. Fraud and Corruption

a. The Bidders/Bidders 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 this RFB, the BMC shall reject a Proposal without being liable in any manner whatsoever to the Bidder, if it determines that the Bidder 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 BMC shall, without prejudice to its any other rights or remedies, forfeit and appropriate the Bid Security or Performance Security, as the case may be, as mutually agreed genuine pre-estimated compensation and damages payable to the Authority for, inter alia, time, cost and effort of the Authority, in regard to the RFB, including consideration and evaluation of such Bidder’s Proposal.

b. Without prejudice to the rights of the BMC under Clause above and the rights and remedies which the BMC may have under the LOI or the Agreement, if an Bidder or Cloud Service Provider, as the case may be, is found by the Authority 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 LOI or the execution of the Agreement, such Bidder or Managed / Cloud Service Provider shall not be eligible to participate in any Bid or RFB

issued by the BMCduring a period of two years from the date such Bidder or Cloud Service Provider, as the case may be, is found by the BMC 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.

The BMC requires that; bidders (applicants/proposers), consultants, contractors and Cloud Service Providers; any sub-contractors, sub-consultants, service providers or Cloud Service Providers; any agents (whether declared or not); and any of their personnel, observe the highest standard of ethics during the procurement process, selection and contract execution of BMC-financed contracts, and refrain from Fraud and Corruption.

a. To this end, the BMC:

Defines, for the purposes of this provision, the terms set forth below as follows:

i. "corrupt practice" means (i) 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 BMC who is or has been associated in any manner, directly or indirectly with the Selection Process or the LOI or has dealt with matters concerning the Agreement or arising there from, 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 BMC, shall be deemed to constitute influencing the actions of a person connected with the Selection Process); or (ii) 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 Project or the LOA or the Agreement, who at any time has been or is a legal, financial or technical consultant/ adviser of the BMC in relation to any matter concerning the Project;

ii. "Fraudulent practice" is any act or omission, including misrepresentation, that knowingly or recklessly misleads, or attempts to mislead, a party to obtain financial or other benefit or to avoid an obligation.

iii. "Collusive practice" is an arrangement between two or more parties designed to achieve an improper purpose, including to influence improperly the actions of another party.

iv. "Coercive practice" is impairing or harming, or threatening to impair or harm, directly or indirectly, any party or the property of the party to influence improperly the actions of a party.

v. "Obstructive practice" is:

(a) deliberately destroying, falsifying, altering, or concealing of evidence material to the investigation or making false statements to investigators in order to materially impede a BMC investigation into allegations of a corrupt, fraudulent, coercive, or collusive practice; and/or threatening, harassing, or intimidating any party to prevent it from disclosing its knowledge of matters relevant to the investigation or from pursuing the investigation; or

(b) acts intended to materially impede the exercise of the BMC's inspection and audit rights provided for under paragraph e. below.

vi. "Undesirable practice" means (i) establishing contact with any person connected with or employed or engaged by BMC with the objective of canvassing, lobbying or in any manner influencing or attempting to influence the Selection Process; or (ii) having a Conflict of Interest; and

vii. "Restrictive practice" means forming a cartel or arriving at any understanding or arrangement among Bidders with the objective of restricting or manipulating a full and fair competition in the Selection Process.

b. Rejects a proposal for award if the BMC determines that the firm or individual recommended for award, any of its personnel, or its agents, or its sub-consultants, sub-contractors, service providers, Cloud Service Providers and/ or their employees, has, directly or indirectly, engaged in corrupt, fraudulent, collusive, coercive, or obstructive practices in competing for the contract in question.
c. In addition to the legal remedies set out in the relevant Legal Agreement, may take other appropriate actions, including declaring mis-procurement, if the BMC determines at any time that representatives of the BMC or of a recipient of any part of the proceeds of the project / subject work engaged in corrupt, fraudulent, collusive, coercive, or obstructive practices during the procurement process, selection and/or execution of the contract in question, without the BMC representative/s having taken timely and appropriate action satisfactory to the BMC to address such practices when they occur, including by failing to inform the BMC in a timely manner at the time they knew of the practices;
d. Pursuant to the BMC's Anti- Corruption Guidelines and in accordance with the BMC's prevailing sanctions policies and procedures, may sanction a firm or individual, either indefinitely or for a stated period of time, including by publicly declaring such firm or individual ineligible (i) to be awarded or otherwise benefit from a BMC-financed contract, financially or in any other manner;(ii) to be a nominated sub-contractor, consultant, manufacturer or Cloud Service Provider, or service provider of an otherwise eligible firm being awarded a BMC-financed contract; and (iii) to participate further in the preparation or implementation of any BMC-financed project;
e. Requires that a clause be included in bidding/request for proposals documents and in contracts financed by BMC, requiring (i) bidders (applicants/proposers), consultants, contractors, and Cloud Service Providers, and their sub-contractors, sub-consultants, service providers, Cloud Service Providers, agents personnel, permit the BMC to inspect all accounts, records and other documents relating to the procurement process, selection and/or contract execution, and to have them audited by auditors appointed by the BMC.

3. Eligible Bidders

a. A Bidder may be a firm that is a private entity, a state-owned entity or institution subject to relevant sub-clause of ITB – Eligible Bidders, or any combination of such entities in the form of a Joint Venture (JV) under an existing agreement or with the intent to enter into such an agreement supported by a letter of intent, if permitted in BDS. In the case of a joint venture, all members shall be jointly and severally liable for the execution of the entire Contract in accordance with the Contract terms. The JV shall nominate a Representative who shall have the authority to conduct all business for and on behalf of any and all the members of the JV during the Bidding process and, in the event the JV is awarded the Contract, during contract execution.

b. A Bidder shall not have a conflict of interest. Any Bidder found to have a conflict of interest shall be disqualified. A Bidder may be considered to have a conflict of interest for the purpose of this Bidding process, if the Bidder:

    i. directly or indirectly controls, is controlled by or is under common control with another Bidder; or

    ii. receives or has received any direct or indirect subsidy from another Bidder; or

    iii. has the same legal representative as another Bidder; or

    iv. has a relationship with another Bidder, directly or through common third parties, that puts it in a position to influence the Bid of another Bidder, or influence the decisions of BMC regarding this Bidding process; or

    v. any of its affiliates participates as a consultant in the preparation of the design or technical specifications of the Cloud Services that are the subject of the Bid; or

    vi. or any of its affiliates has been hired (or is proposed to be hired) by BMC for the Contract implementation; or

vii. would be providing goods, works, or non-consulting services resulting from or directly related to consulting services for the preparation or implementation of the project that it provided or were provided by any affiliate that directly or indirectly controls, is controlled by, or is under common control with that firm; or

viii. has a close business or family relationship with a professional staff of the BMC who: (i) are directly or indirectly involved in the preparation of the bidding document or specifications of the contract, and/or the Bid evaluation process of such contract; or (ii) would be involved in the implementation or supervision of such contract unless the conflict stemming from such relationship has been resolved in a manner acceptable to the BMC throughout the procurement process and execution of the Contract.

c. A firm that is a Bidder (either individually or as a JV member) shall not participate in more than one Bid. This includes participation as a subcontractor. Such participation shall result in the disqualification of all Bids in which the firm is involved. A firm that is not a Bidder or a JV member, may participate as a sub-contractor in more than one Bid.

d. A Bidder that has been sanctioned/banned/blacklisted by the BMC, shall be ineligible to be prequalified for, initially selected for, bid for, propose for, or be awarded a BMC-financed contract or benefit from a BMC-financed contract, financially or otherwise, during such period of time as the BMC shall have determined. The list of debarred firms and individuals is available at the office of Central Purchase Department of BMC.

e. Bidders that are state-owned enterprises or institutions in India may be eligible to compete and be awarded a Contract(s) only if they can establish, in a manner acceptable to the BMC, that they: (i) are legally and financially autonomous; (ii) operate under commercial law; and (iii) are not under supervision of BMC.

f. A Bidder shall provide such documentary evidence of eligibility satisfactory to BMC, as BMC shall reasonably request.

4. Qualification of the Bidder

All Bidders shall provide information as per Section – Evaluation & Qualification Criteria, a preliminary description of the proposed work method and schedule, including drawings and charts, as necessary.

5. Code of integrity

No official of a procuring entity or a bidder shall act in contravention of the codes which includes

a. prohibition of

i. Making offer, solicitation or acceptance of bribe, reward or gift or any material benefit, either directly or indirectly, in exchange for an unfair advantage in the procurement process or to otherwise influence the procurement process.

ii. Any omission, or misrepresentation that may mislead or attempt to mislead so that financial or other benefit may be obtained, or an obligation avoided.

iii. Any collusion, bid rigging or anticompetitive behavior that may impair the transparency, fairness and the progress of the procurement process.

iv. Improper use of information provided by the procuring entity to the bidder with an intent to gain unfair advantage in the procurement process or for personal gain.

v. Any financial or business transactions between the bidder and any official of the procuring entity related to tender or execution process of contract, which can affect the decision of the procuring entity directly or indirectly.

vi. Any coercion or any threat to impair or harm, directly or indirectly, any party or its property to influence the procurement process.

vii. Obstruction of any investigation or auditing of a procurement process.

viii. Making false declaration or providing false information for participation in a tender process or to securecontract.

b. Disclosure of conflict of interest.

c. Disclosure by the bidder of any previous transgressions made in respect of the provisions of sub-clause (a) with any entity in any country during the last three years or of being debarred by any other procuring entity.

In case of any reported violations, the procuring entity, after giving a reasonable opportunity of being heard, comes to the conclusion that a bidder or prospective bidder, as the case may be, has contravened the code of integrity, may take appropriate measures.

B. Contents of Bidding Document

6. Sections of Bidding Document

a. The bidding document consists of Parts 1 and 2, which include all the sections indicated below, and should be read in conjunction with any Addenda issued if any.

b. **PART 1: Bidding Procedures**

i. Section I - Instructions to Bidders (ITB)

ii. Section II - Bid Data Sheet (BDS)

iii. Section III - Evaluation and Qualification Criteria

iv. Section IV – Bidding Forms

c. **PART 2: BMC's Project Requirements**

i. Section V - BMC's Project Requirements

1. Background and Informational Materials

2. Technical Requirements

3. Implementation Schedule

4. System Inventory Tables

ii. Section VI - General Conditions of Contract (GCC)

d. The Bid Notice - Request for Bids (RFB) issued by BMC is not part of this bidding document.

e. Unless obtained directly from Mahatenders website, BMC is not responsible for the completeness of the document, responses to requests for clarification, the Minutes of the pre-Bid meeting (if any), or Addenda to the bidding document. In case of any contradiction, documents obtained directly from BMC shall prevail.

f. The Bidder is expected to examine all instructions, forms, terms, and specifications in the bidding document and to furnish with its Bid all information or documentation as is required by the bidding document.

7. Clarification of Bidding Document, Site Visit, Pre-bid Meeting

a. A Bidder requiring any clarification of the bidding document shall contact the BMC in writing at the BMC's address specified in the Notice Inviting Tender (NIT) or raise its enquiries during the pre-Bid meeting if provided for in accordance with this ITB. If so, specified in the Notice Inviting Tender (NIT), the BMC shall also promptly publish its response at the web page identified in the Notice Inviting Tender (NIT). Should the BMC deem it necessary to amend the bidding document as a result of a request for clarification, it shall do so following the procedure under ITB - Amendment of Bidding Document and ITB - Deadline for Submission of Bids.

b. The Bidder may wish to visit and examine the site where the Cloud Servicesare to be installed and / or provide user support / handholding, its surroundings and obtain for itself on its own responsibility all information that may be necessary for preparing the Bid and entering into a contract. The costs of visiting the site shall be at the Bidder's own expense.

c. The Bidder and any of its personnel or agents will be granted permission by the BMC to enter upon its premises and lands for the purpose of such visit, but only upon the express condition that the Bidder, its personnel, and agents will release and indemnify the BMC and its personnel and agents from and against all liability in respect thereof, and will be responsible for death or personal injury, loss of or damage to property, and any other loss, damage, costs, and expenses incurred as a result of the inspection.

d. The Bidder's designated representative is invited to attend a pre-Bid meeting and/or a site visit, if provided for in the Bid Notice. The purpose of the meeting will be to clarify issues and to answer questions on any matter that may be raised at that stage.

e. The Bidder is requested, as far as possible, to submit any questions in writing, to reach the BMC not later than one week before the meeting.

f. Minutes of the pre-Bid meeting, including the text of the questions raised without identifying the source, and the responses given, together with any responses prepared after the meeting, will be published promptly on the website URL mentioned in the BDS. Any modification to the bidding document that may become necessary as a result of the pre-Bid meeting shall be made by the BMC exclusively through the issue of an Addendum pursuant to ITB - Amendment of Bidding Document and not through the minutes of the pre-Bid meeting.

g. Non-attendance at the pre-Bid meeting will not be a cause for disqualification of a Bidder.

8. Amendment to the Bidding Document

a. At any time prior to the deadline for submission of Bids, BMC may amend the bidding document by issuing addenda\ corrigendum.

b. BMC shall publish the addendum\ corrigendum on e-Tendering website and any addendum\ corrigendum issued shall be part of the bidding document.

c. To give prospective Bidders reasonable time in which to take an addendum into account in preparing their Bids, the BMC may, at its discretion, extend the deadline for the submission of Bids, pursuant to ITB - Deadline for Submission of Bids.

C. Preparation of Bids

9. Cost of Bidding

a. The Bidder shall bear all costs associated with the preparation and submission of its Bid, and BMC shall not be responsible or liable for those costs, regardless of the conduct or outcome of the Bidding process.

10. Language of Bid

a. The Bid as well as all correspondence and documents relating to the Bid exchanged by the Bidder and BMC shall be written in English language. Supporting documents and printed literature that are part of the Bid may be in another language provided they are accompanied by an accurate translation of the relevant passages into English language, in which case, for purposes of interpretation of the Bid, such translation shall govern.

11. Documents Comprising the Bid

a. The Bid shall comprise the following:

i. Letter of Bid prepared in accordance with ITB - Letter of Bid and Price Schedule;

ii. **Price Schedules** completed in accordance with ITB - Letter of Bid and Price Schedule and ITB Bid Prices;

iii. **Bid Security or Bid-Securing Declaration** in accordance with ITB - Bid Security;

iv. **Authorization:** written confirmation authorizing the signatory of the Bid to commit the Bidder, in accordance with ITB - Format and Signing of Bid. Written confirmation may include resolution of the Board of Directors of the Company authorizing the signatory of the Bid to commit the Bidder or Power of Attorney executed by the Bidder in favor of the signatory of the Bid;

v. **Bidder's Eligibility**: documentary evidence in accordance with ITB - Documents Establishing the Eligibility and Qualifications of the Bidder establishing the Bidder's eligibility and qualifications to perform the contract if its Bid is accepted;

vi. **Conformity**: documentary evidence established in accordance with ITB - Documents Establishing Conformity that the Cloud Services offered by the Bidder conform to the bidding document;

vii. **Sub-contractors:** list of subcontractors, in accordance with ITB - Documents Establishing Conformity of the Cloud Services;

viii. **Intellectual Property**: a list of: Intellectual Property all Software included in the Bid;

ix. Any other document required in the BDS (if mentioned) and / or required as part of the Bid.

b. In addition to the above requirements, Bids submitted by a JV shall include a copy of the Joint Venture Agreement entered into by all members indicating at least the parts of the Cloud Services to be executed by the respective members. Alternatively, a letter of intent to execute a Joint Venture Agreement in the event of a successful Bid shall be signed by all members and submitted with the Bid, together with a copy of the proposed Agreement indicating at least the parts of the Cloud Services to be executed by the respective members.

12. Letter of Bid and Price Schedule

a. The Letter of Bid and all other formats including filled in Price Schedule shall be prepared using the relevant forms furnished in Section – Bidding Forms. The forms must be completed without any alterations to the text, and no substitutes shall be accepted. All blank spaces shall be filled in with the information requested.

13. Alternative Bids

a. Alternative Bids shall not be considered.

14. Documents Establishing the Eligibility and Qualifications of the Bidder

a. To establish its eligibility and qualifications to perform the Contract in accordance with Section - Evaluation and Qualification Criteria, the Bidder shall provide the information requested in the corresponding information sheets included in Section - Bidding Forms.

b. In the event that prequalification of potential Bidders has been undertaken as stated in the BDS, only Bids from prequalified Bidders shall be considered for award of Contract.

15. Documents Establishing Conformity of the Cloud Services

a. Pursuant to ITB – Documents Comprising the Bid, the Bidder shall furnish, as part of its Bid documents establishing the conformity to the bidding documents of the Cloud Services that the Bidder proposes to design, supply and install under the Contract

b. The documentary evidence of conformity of the Cloud Services to the bidding documents including:

   i. Preliminary Project Plan describing, among other things, the methods by which the Bidder will carry out its overall management and coordination responsibilities if awarded the Contract, and the human and other resources the Bidder proposes to use. The Preliminary Project Plan must also address any other topics specified in the Bid Document. In addition, the Preliminary Project Plan should state the Bidder's assessment of what it expects the BMC and any other party involved in the implementation of the Cloud Services to provide during implementation and how the Bidder proposes to coordinate the activities of all involved parties;

   ii. written confirmation that the Bidder accepts responsibility for the successful integration and inter-operability of all components of the Cloud Services as required by the bidding documents;

   iii. an item-by-item commentary on the BMC's Technical Requirements, demonstrating the substantial responsiveness of the Cloud Services offered to those requirements. In demonstrating responsiveness, the Bidder is encouraged to use the Technical Responsiveness Checklist (or Checklist Format) in the Sample Bidding Forms (Section - Bidding Forms). The commentary shall include explicit cross-references to the relevant pages in the supporting materials included in the bid. Whenever a discrepancy arises between the item-by-item commentary and any catalogs, technical specifications, or other preprinted materials submitted with the bid, the item-by-item commentary shall prevail;

   iv. support material (e.g., product literature, white papers, narrative descriptions of technologies and/or technical approaches), as required and appropriate; and

   v. any separate and enforceable contract(s) for Recurrent Cost items which the BDS ITB – Bid Prices required Bidders to bid.

c. References to brand names or model numbers or national or proprietary standards designated by the BMC in the bidding documents are intended to be descriptive and notecht restrictive. The Bidder may substitute alternative brand/model names or standards in its bid, provided that it demonstrates to the BMC's satisfaction that the use of the substitute(s) will result in the Cloud Services being able to perform substantially equivalent to or better than that specified in the Technical Requirements.

d. For major items of the Cloud Services as listed by the BMC in Section - Evaluation and Qualification Criteria, which the Bidder intends to purchase or subcontract, the Bidder shall give details of the name and nationality of the proposed subcontractors, including manufacturers, for each of those items. In addition, the Bidder shall include in its Bid information establishing compliance with the requirements specified by the BMC for these items. Quoted rates and prices will be deemed to apply to whichever subcontractor is appointed, and no adjustment of the rates and prices will be permitted.

e. **If Sub-Contracting, Cost of sub-contractor shall not exceed 25% of Total Contract cost**.

f. The Bidder shall be responsible for ensuring that any subcontractor proposed complies with the requirements of ITB – Eligible Bidder, and that any goods or services to be provided by the subcontractor comply with the requirements of this ITB.

16. Bid Prices

a. All Goods and Services identified in the Section – BMC's Requirements, and all other Goods and Services proposed by the Bidder to fulfill the requirements of the Cloud Services, must be priced in the corresponding commercial bid, in accordance with the instructions provided in the manner specified below.

b. The Bidder must also bid Recurrent Cost Items specified in the Technical Requirements, in Section – BMC's Requirements (if any). These must be priced separately in the corresponding commercial bid, in accordance with the instructions provided in the tables and in the manner specified below:

   i. prices for Recurrent Costs are all-inclusive of the costs of necessary Goods such as spare parts, software license renewals, labor, etc., needed for the continued and proper operation of the Cloud Services and, if appropriate, of the Bidder's own allowance for price increases;

   ii. Prices for Recurrent Costs beyond the scope of warranty services to be incurred during the Warranty Period, defined in GCC Clause – Defect Liability shall be quoted as Service prices on the Recurrent Cost Sub-Table in detail.

c. Bidders may be required to provide a breakdown of any composite or lump-sum items included in the Cost Tables

d. The price of items that the Bidder has left blank in the cost tables provided in the commercial bid shall be assumed to be included in the price of other items. Items omitted altogether from the cost tables shall be assumed to be omitted from the bid and, the bid in such case shall be treated as non-responsive.

e. The prices must include all costs incidental to the performance of the Services, as incurred by the Bidder, such as travel, subsistence, office support, communications, translation, printing of materials, etc. Costs incidental to the delivery of the Services but incurred by the BMC or its staff, or by third parties, must be included in the price only to the extent such obligations are made explicit in these bidding documents (as, e.g., a requirement for the Bidder to include the travel and subsistence costs of trainees).

f. The prices quoted by the Bidder shall be fixed during the Bidder's performance of the Contract and not subject to increases on any account. Bids submitted that are subject to price adjustment will be rejected.

17. Currencies of Bid and Payment

a. The currency(ies) of the Bid and currencies of payment shall be the same. The Bidder shall quote in the currency of Indian Rupee (INR).

18. Period of Validity of Bids

a. Bids shall remain valid for the period specified in the BDS after the Bid submission deadline prescribed by the BMC in accordance with ITB - Deadline for Submission of Bids. A Bid valid for a shorter period shall be rejected by the BMC as nonresponsive.

b. In exceptional circumstances, prior to the expiration of the Bid validity period, the BMC may request Bidders to extend the period of validity of their Bids. The request and the responses shall be made in writing. If a Bid Security is requested in accordance with ITB – Bid Security, it shall also be extended for thirty days (30) beyond the deadline of the extended validity period. A Bidder may refuse the request without forfeiting its Bid

Security. A Bidder granting the request shall not be required or permitted to modify its Bid**.**

19. Bid Security

a. The Bidder shall furnish as part of its Bid, a Bid Security as specified **in the Bid Notice / E-Procurement Notice**, in the amount and currency specified in the **Bid Notice / E-Procurement Notice.**

b. If a Bid Security is specified pursuant to this ITB, any Bid not accompanied by a substantially responsive Bid Security shall be rejected by the BMC as non-responsive.

c. If a Bid Security is specified pursuant to this ITB, the Bid Security of unsuccessful Bidders shall be returned as promptly as possible upon the successful Bidder's furnishing of the Performance Security pursuant to ITB

– **Performance Security.**

d. The Bid Security of the successful Bidder shall be returned as promptly as possible once the successful Bidder has signed the Contract and furnished the required Performance Security.

e. The Bid Security may be forfeited:

i. if a Bidder withdraws its Bid during the period of Bid validity specified by the Bidder on the Letter of Bid; or

ii. if the successful Bidder fails to:

1. sign the Contract in accordance with ITB – Signing of Contract; or

2. Furnish performance security in accordance with ITB – Performance Security.

f. The Bid Security of a JV shall be in the name of the JV that submits the bid. If the JV has not been legally constituted into a legally enforceable JV at the time of Bidding, the Bid Security or the Bid-Securing Declaration shall be in the names of all future members as named in the letter of intent referred to in ITB – Eligible Bidders and ITB – Documents Comprising the Bid.

g. If a Bid Security is not required **in the BDS, and**;

i. if a Bidder withdraws its Bid during the period of Bid validity specified by the Bidder on the Letter of Bid Form, except as provided in ITB – Period of Validity of Bids; or

ii. if the successful Bidder fails to: sign the Contract in accordance with ITB – Signing of Contract; or furnish a Performance Security in accordance with ITB – Performance Security;

the BMC may, if provided for in the BDS, declare the Bidder disqualified to be awarded a contract by the BMC for a period of time as stated in the BDS.

20. Format and Signing of Bid

a. The Bid shall be digitally signed by a person duly authorized to sign on behalf of the Bidder, using Digital Signature issued by authorized Certifying Authority. This authorization shall consist of written confirmation and shall be attached to the Bid. The name and position held by the person signing the authorization must be typed or printed below the signature. All scanned pages of the Bid where entries or amendments have

been made shall be signed or initialed by the person signing the Bid and submitted on e-Tendering system of BMC.

b. In case the Bidder is a JV, the Bid shall be digitally signed by an authorized representative of the JV on behalf of the JV, and so as to be legally binding on all the members as evidenced by a power of attorney signed by their legally authorized representatives.

D. Submission and Opening of Bids

21. Submission of Bids

a. The Bid documents listed above shall be submitted in three folders as following:

i. Cover 1 / Fee- Documentary Evidence of Online Payment of Tender Fee and Bid Security (EMD) on e-Tendering System.

ii. Cover 2 / Pre-Qual& Technical-Letter of Bid, Authorization, Bidder's Eligibility, Documentary evidence of Qualifications and Conformity`

iii. Cover 3 / Finance- Price Schedule to be duly filled in the online form of commercial offer on e-Tendering System of BMC, Financial Cover Letter .**Bidder shall NOT disclose the rates / prices quoted in any other Bid document.**

22. Deadline for Submission of Bids

a. Bids must be received by BMC on e-Tendering system no later than the date and time specified **in the Bid Notice / E-Procurement Notice**.

b. BMC may, at its discretion, extend the deadline for the submission of Bids by amending the bidding document, in which case all rights and obligations of BMC and Bidders previously subject to the deadline shall thereafter be subject to the deadline as extended.

23. Late Bids

a. BMC shall not consider any Bid that arrives after the deadline for submission of Bids, in accordance **with ITB –** Deadline for Submission of Bids. Any Bid received by BMC after the deadline for submission of Bids shall be declared late and rejected.

24. Withdrawal, Substitution and Modification of Bids

a. A Bidder may withdraw, substitute, or modify its Bid after it has been submitted, prior to the deadline prescribed for submission of Bids, in accordance with ITB – Deadline for Submission of Bids.

b. No Bid may be withdrawn, substituted, or modified in the interval between the deadline for submission of Bids and the date of expiry of the Bid validity specified in the BDS or any extended date thereof. Withdrawal of a bid during this interval may result in the forfeiture of the Bidder's Bid Security.

25. Bid Opening

a. BMC shall conduct the Bid opening in public, in the presence of Bidders` designated representatives and anyone who chooses to attend, and at the address, date and time specified in the BDS.

b. The BMC shall neither discuss the merits of any Bid nor reject any Bid.

c. The BMC shall prepare a record of the Bid opening that shall include, as a minimum:

i. the Bid Price, per lot if applicable, including any discounts;

ii. the presence or absence of a Bid Security

d. The Bidders' representatives who are present shall be requested to sign the record. The omission of a Bidder's signature on the record shall not invalidate the contents and effect of the record. A copy of the record shall be distributed to all Bidders.

E. Evaluation and Comparison of Bids

26. Confidentiality

a. Information relating to the evaluation of Bids and recommendation of contract award, shall not be disclosed to Bidders or any other persons not officially concerned with the Bidding process until information on the Intention to Award the Contract is published.

b. Any effort by a Bidder to influence BMC in the evaluation or contract award decisions may result in the rejection of its Bid.

c. Notwithstanding in this clause, from the time of Bid opening to the time of Contract Award, if any Bidder wishes to contact BMC on any matter related to the Bidding process, it should do so in writing.

27. Clarification of Bids

a. To assist in the examination, evaluation, and comparison of Bids, and qualification of the Bidders, BMC may, at BMC's discretion, ask any Bidder for clarification of its Bid including breakdowns of the prices in the Price Schedule, and other information that BMC may require. Any clarification submitted by a Bidder in respect to its Bid and that is not in response to a request by BMC shall not be considered. BMC's request for clarification and the response shall be in writing. No change, including any voluntary increase or decrease, in the prices or substance of the Bid shall be sought, offered, or permitted.

b. Maximum 5 shortfalls of curable defects shall be allowed and in case, curable defects are not complied by bidder within given time period, the bidder shall be treated as non-responsive and such cases will be informed to Registration and Monitoring cell. Such non-submission of documents will be considered as 'Intentional Avoidance' and if three or more cases in 12 months are reported, shall be viewed seriously and disciplinary action against the defaulters such as banning/deregistration, etc. shall be taken by Registration Cell with due approval of the concerned AMC.

c. If a Bidder does not provide clarifications of its Bid by the date and time set in BMC's request for clarification which is three days from the date of BMC's request letter, its Bid may be rejected.

28. Deviations, Reservations, Omission, Curable and Non-curable Defects

a. During the evaluation of Bids, the following definitions apply:

   i. "Deviation" is a departure from the requirements specified in the bidding document;

   ii. "Reservation" is the setting of limiting conditions or withholding from complete acceptance of the requirements specified in the bidding document; and

   iii. "Omission" is the failure to submit part, or all of the information or documentation required in the bidding document.

   iv. "Curable Defect" shall mean shortfalls in submission such as:

      1. non-submission of following documents

a. Valid Registration Certificate

b. Valid Bank Solvency

c. GST Registration Certificate

d. Certified Copies of PAN documents and photographs of individuals, owners, etc.

e. Partnership Deed and any other documents

f. Undertakings as mentioned in the tender document.

2. Wrong calculation of Bid Capacity,

v. "Non-curable" Defect shall mean

1. In-adequate submission of EMD/ASD amount,

2. In-adequacy of technical and financial capacity with respect to Eligibility criteria as stipulated in the tender

29. Determination of Responsiveness

a. BMC's determination of a Bid's responsiveness is to be based on the contents of the Bid itself, as defined in ITB – Documents Comprising the Bid.

b. A substantially responsive Bid is one that meets the requirements of the bidding document without material deviation, reservation, or omission. A material deviation, reservation, or omission is one that:
   i. if accepted, would:
      1. affect in any substantial way the scope, quality, or performance of the Services specified in the Contract; or
      2. limit in any substantial way, inconsistent with the bidding document, BMC's rights or the Bidder's obligations under the Contract; or
   ii. if rectified, would unfairly affect the competitive position of other Bidders presenting substantially responsive Bids.

c. BMC shall examine the technical aspects of the Bid submitted in accordance with ITB - Documents Establishing Conformity of Services and ITB - Documents Establishing the Eligibility and Qualifications of the Bidder, in particular, to confirm that all requirements of Section - BMC's Requirements have been met without any material deviation or reservation, or omission.

d. To be considered for Contract award, Bidders must have submitted Bids:
   i. for which detailed Bid evaluation using the same standards for compliance determination as listed in ITB - Deviations, Reservations, and Omissions and this ITB confirms that the Bids are commercially and technically responsive, and include the hardware, Software, related equipment, products, Materials, and other Goods and Services components of the Cloud Services in substantially the full required quantities for the entire Cloud Services, the individual Subsystem; and are deemed by the BMC as commercially and technically responsive; and
   ii. that offer Information Technologies that are proven to perform up to the standards promised in the bid by having successfully passed the performance, benchmark, and/or functionality tests the BMC may require, pursuant to ITB Eligibility and Qualification of the Bidder.

30. Nonconformities, Errors, and Omissions

a. Provided that a Bid is substantially responsive, the BMC may waive any nonconformity in the Bid that does not constitute a material deviation, reservation, or omission.

b. Provided that a Bid is substantially responsive, BMC may request that the Bidder submit the necessary information or documentation, within a reasonable period of time, to rectify nonmaterial nonconformities in the Bid related to documentation requirements. Requesting information or documentation on such nonconformities shall not be related to any aspect of the price of the Bid. Failure of the Bidder to comply with the request may result in the rejection of its Bid.

31. Evaluation of Bids

a. The BMC shall use the criteria and methodologies listed in this ITB and Section - Evaluation and Qualification criteria. No other evaluation criteria or methodologies shall be permitted. By applying the criteria and methodologies the BMC shall determine the responsive bids.

b. **Preliminary Examination**

i. The BMC will examine the bids, to determine whether required sureties have been furnished, and are substantially complete (e.g., not missing key parts of the bid or silent on excessively large portions of the Technical Requirements).

c. **Technical Evaluation**

i. The BMC will examine the information supplied by the Bidders Pursuant to ITB – Documents Comprising the Bid and ITB – Documents Comprising the Conformity of the Cloud Services, and in response to other requirements in the Bidding document, taking into account the following factors:

1. overall completeness and compliance with the Technical Requirements; and deviations from the Technical Requirements.
2. suitability of the Cloud Services offered in relation to the conditions prevailing at the site; and the suitability of the implementation and other services proposed, as described in the Preliminary Project Plan included in the bid;
3. achievement of specified performance criteria by the Cloud Services;
4. compliance with the time schedule called for by the Implementation Schedule and any alternative time schedules offered by Bidders, as evidenced by a milestone schedule provided in the Preliminary Project Plan included in the bid;
5. type, quantity, quality, and long-term availability of maintenance services and of any critical consumable items necessary for the operation of the Cloud Services;
6. any other relevant technical factors that the BMC deems necessary or prudent to take into consideration;
7. any proposed deviations in the bid to the contractual and technical provisions stipulated in the bidding documents.

ii. If specified in the BDS, the BMC's evaluation of responsive Bids will take into account technical factors, in addition to cost factors. An Evaluated Bid Score (B) will be calculated for each responsive Bid using the formula, specified in Section - Evaluation and Qualification Criteria, which permits a comprehensive assessment of the Bid cost and the technical merits of each Bid

d. **Economic (Commercial) Evaluation**

i. **To evaluate a Bid, the BMC shall consider the following:**

1. The Bid price, quoted by the bidder inclusive of all taxes (except GST), duties, levies and fees.

e. The BMC will evaluate and compare the Bids that have been determined to be substantially responsive, pursuant to ITB – Determination of Responsiveness. The evaluation will be performed assuming that theContract will be awarded to the technically responsive and commercially lowest bidder for the entire Cloud Services;

32. Comparison of Bids

a. BMC shall compare the evaluated costs of all substantially responsive Bids established in accordance with ITB – Evaluation of Bids to determine the Bid that has the lowest evaluated cost.

33. Abnormally Low Bids

a. An Abnormally Low Bid is one where the Bid price, in combination with other constituent elements of the Bid, appears unreasonably low (as defined in BDS) to the extent that the Bid price raises material concerns as to the capability of the Bidder to perform the Contract for the offered Bid price.

b. In the event of identification of a potentially Abnormally Low Bid, BMC shall seek written clarifications from the Bidder, including detailed price analyses of its Bid price in relation to the subject matter of the contract, scope, proposed methodology, schedule, allocation of risks and responsibilities and any other requirements of the bidding document.

c. After evaluation of the price analyses, in the event that BMC determines that the Bidder has failed to demonstrate its capability to perform the Contract for the offered Bid Price, BMC shall reject the Bid.

34. Eligibility and Qualification of the Bidder

a. BMC shall determine to its satisfaction whether the Bidder that is selected as having submitted the lowest evaluated cost and substantially responsive Bid is eligible and meets the qualifying criteria specified in **Section - Evaluation and Qualification Criteria.**

b. The determination shall be based upon an examination of the documentary evidence of the Bidder's qualifications submitted by the Bidder, pursuant to ITB -Documents Establishing the Eligibility and Qualifications of the Bidder. The determination shall not take into consideration the qualifications of other firms such as the Bidder's subsidiaries, parent entities, affiliates, subcontractors, or any other firm(s) different from the Bidder that submitted the Bid.

c. Prior to Contract award, BMC will verify that the successful Bidder (including each member of a JV) is not disqualified by BMC due to noncompliance with any other contractual obligations. BMC will conduct the same verification for each subcontractor proposed by the successful Bidder. If any proposed subcontractor does not meet the requirement, BMC shall reject the Bid.

d. An affirmative determination shall be a prerequisite for award of the Contract to the Bidder. A negative determination shall result in disqualification of the Bid, in which event BMC shall proceed to the Bidder who offers a substantially responsive Bid with the next lowest evaluated cost to make a similar determination of that Bidder's qualifications to perform satisfactorily.

35. BMC's Right to Accept Any Bid, and to Reject Any or All Bids

a. BMC reserves the right to accept or reject any Bid, and to annul the Bidding process and reject all Bids at any time prior to Contract Award, without thereby incurring any liability to Bidders. In case of annulment, all Bids submitted and specifically, Bid securities, shall be promptly returned to the Bidders.

F. Award of Contract

36. Award Criteria

a. Subject to ITB - BMC's Right to Accept Any Bid, and to Reject Any or All Bids, BMC shall award the Contract to the successful Bidder. This is the Bid of the Bidder that meets the qualification criteria and whose Bid has been determined to be:

i. substantially responsive to the bidding document; and

ii. the lowest evaluated cost.

37. Notification of Award

a. Prior to the date of expiry of the Bid validity, or any extension thereof, BMC shall notify the successful Bidder, in writing, that its Bid has been accepted. The notification of award (hereinafter and in the Conditions of Contract and Contract Forms called the “Letter of Acceptance”) shall specify the sum that BMC will pay the Managed / Cloud Service Provider in consideration of the execution of the Contract (hereinafter and in the Conditions of Contract and Contract Forms called “the Contract Price”).

b. Until a formal Contract is prepared and executed, the Letter of Acceptance shall constitute a binding Contract.

38. Signing of Contract

a. BMC shall send to the successful Bidder the Letter of Acceptance including the Contract Agreement.

b. The successful Bidder shall sign, date and return to BMC, the Contract Agreement within thirty (30) days of its receipt, **failing which a penalty of Rs. 5000/- per day will be applicable** to the bidder

39. Failure to Agree with the Terms and Conditions of the RFB

Failure of the successful Bidder to agree with the Draft Legal Agreement and Terms & Conditions of the RFB shall constitute sufficient grounds for the annulment of the award, in which event BMC may award the contract to the next best value Bidder or call for new proposals from the interested Bidders.

In such a case, the BMC shall forfeit the Bid Security of the selected Bidder.

40. Performance Security

a. Within thirty (30) days of the receipt of the Letter of Acceptance from BMC, the successful Bidder shall furnish the Performance Security in accordance with the relevant GCC,**failing which a penalty of Rs. 5000/- per day will be applicable** to the bidder, using for that purpose the Performance Security Form included in Section – Bidding Forms. The Performance Security shall be valid for a period as mentioned **in BDS**.

b. Failure of the successful Bidder to submit the above-mentioned Performance Security or sign the Contract shall constitute sufficient grounds for the annulment of the award and forfeiture of the Bid Security. In that event BMC may award the Contract to the Bidder offering the next Most Advantageous Bid.

41. Legal, Stationery Charges & Stamp Duty

a. Within thirty (30) days of the receipt of the Letter of Acceptance from BMC, the successful Bidder shall furnish the Legal & Stationery Charges, using for that purpose the table given in Section – Bidding Forms or revised Legal and Stationery Charges published by BMC from time to time and effective on the date of issuance of the Notification of Award. The successful Bidder shall note that stationery charges as given in the relevant table shall be

recovered from the successful Bidder for supply of requisite prescribed forms for preparing certificate bills in respect of the work.

b. Within thirty (30) days of the receipt of the Letter of Acceptance from BMC, the successful Bidder shall pay Stamp Duty, in accordance with the provisions of Article 63, Schedule I of Bombay Stamp Act 1958, using for that purpose the table given in Section – BiddingForms or revised Stamp Duty Charges published by the Government from time to time and effective on the date of issuance of the Notification of Award.

c. BMC shall recover shortfall if any, in the amount of Stamp Duty paid by the successful Bidder and shall deposit the shortfall amount to Superintendent of Stamp, Mumbai within fifteen (15) days from the intimation of notice of short payment of Stamp Duty.

42. BMC's Right to Vary Quantities at Time of Award

a. BMC reserves the right at the time of Contract award to increase or decrease, by the twenty (20) percentage(s) for items as indicated in the Price Schedule.

43. Grievance Redressal Mechanism

BMC has formed a Grievance Redressal Mechanism for redressal of Bidder's grievances. Any Bidder or prospective Bidder aggrieved by any decision, action or omission of the procuring entity being contrary to the provisions of the tender or any rules or guidelines issued therein, in Packet 'A', 'B' & 'C' can make an application for review of decision of responsiveness in Packet 'A', 'B' & 'C' within a period of 7 days or any such other period, as may be specified in the Bid document.

While making such an application to procuring entity for review, aggrieved Bidders or prospective bidders shall clearly specify the ground or grounds in respect of which he feels aggrieved.

Provided that after declaration of a bidder as a successful in Packet 'A' (Pre-Qual/General Requirements), an application for review may be filed only by a bidder who has participated in procurement proceedings and after declaration of successful bidders in Packet 'B' (Technical Bid), an application for review may be filed only by successful bidders of Packet 'A'. Provided further that, an application for review of the financial bid can be submitted, by the bidder whose technical bid is found to be acceptable / responsive.

Upon receipt of such application for review, BMC may decide whether the bid process is required to be suspended pending disposal of such review. The BMC after examining the application and the documents available to him, give such reliefs, as may be considered appropriate and communicate its decision to the Applicant and if required to other bidders or prospective bidders, as the case may be.

BMC shall deal and dispose of such applications as expeditiously as possible and in any case within 10 days from the date of receipt of such application or such other period as may be specified in pre-qualification document, bidder registration document or bid documents, as the case may be.

Where BMC fails to dispose of the application within the specified period or if the bidder or prospective bidder feels aggrieved by the decision of the procuring entity, such bidder or prospective bidder may file an application for redressal before the "Internal Procurement Redressal Committee" within 7 days of the expiry of the allowed time or of the date of receipt of the decision, as the case may be. Every such application for internal redressal before Redressal Committee shall be accompanied by fee of Rs. 25,000/- and fees shall be paid in the form of D.D. in favor of BMC.

1st Appeal by the bidder against the decision of C.E. / HOD / Dean can be made to concerned DMC / Director who should decide appeal in 7 days.

If not satisfied, 2nd Appeal by the bidder can be made to concerned A.M.C. for decision.

Grievance Redressal Committee (GRC) is headed by concerned D.M.C. / Director of particular department for the first appeal / grievances by the bidder against the decision for responsiveness / non responsiveness in Packet 'A', Packet 'B' or Packet 'C' and if not satisfied, concerned A.M.C. will take decision as per second appeal made by the bidder.

This Grievance Redressal Committee (GRC) will be operated through DMC (CPD) office where appeals of aggrieved bidder will be received with fee of Rs. 25,000/- from aggrieved bidder. The necessary correspondence in respect of said applications to the aggrieved bidder & concerned department, issuing notices, arranging of Grievance Redressal Committee (GRC) with D.M.C. and further proceeding will be carried out through registrar appointed by BMC.

No application shall be maintainable before the redressal committee in regard of any decision of the BMC relating to following issues

Determination of need of procurement

The decision of whether or not to enter into negotiations

Cancellation of a procurement process for certain reasons

On receipt of recommendation of the committee, it will be communicate his decision there on to the Applicant within 10 days or such further time not exceeding 20 days, as may be considered necessary from the date of receipt of the recommendation and in case of non-acceptance of any recommendation, the reason for such non acceptance shall also be mentioned in such communication.

Additional Municipal Commissioner and / or Grievance Redressal Committee, if found, come to the conclusion that any such complaint or review is of vexatious, frivolous or malicious nature and submitted with the intention of delaying or defeating any procurement or causing loss to the procuring entity or any other bidder, then such complainant shall be punished with fine, which may extend to Five Lac rupees or two percent of the value of the procurement, whichever is higher.

44. Disclaimer

The information contained in this e-tender document or provided to Bidder(s), whether verbally or in documentary or any other form, by or on behalf of the Brihanmumbai Municipal Corporation(BMC), hereafter also referred as “The BMC Authority “, or any of its employees or advisors, is provided to Bidder(s) on the terms and conditions set out in this e-tender and such other terms and conditions subject to which such information is provided.

This e-tender includes statements, which reflect various assumptions and assessments arrived at by the Brihanmumbai Municipal Corporation(BMC) in relation to the Project. Such assumptions, assessments and statements do not purport to contain all the information that each Bidder may require. This e-tender may not be appropriate for all persons, and it is not possible for the Brihanmumbai Municipal Corporation(BMC), its employees or advisors to consider the investment objectives, financial situation and particular needs of each party who reads or uses this e-tender. The assumptions, assessments, statements, and information contained in this e-tender may not be complete, accurate, adequate or correct. Each Bidder should, therefore, conduct its own investigations and analysis and should check the accuracy, adequacy, correctness, reliability and completeness of the assumptions, assessments, statements and information contained in this e-tender and obtain independent advice from appropriate sources.

Information provided in this e-tender to the Bidder(s) is on a wide range of matters, some of which may depend upon interpretation of law. The information given is not intended to be an exhaustive account of statutory requirements and should not be regarded as a complete or authoritative statement of law. The Brihanmumbai Municipal Corporation (BMC) accepts no responsibility for the accuracy or otherwise for any interpretation or opinion on law expressed here.

The Brihanmumbai Municipal Corporation(BMC), its employees and advisors make no representation or warranty and shall have no liability to any person, including any Bidder or Bidder, under any law, statute, rules or regulations or tort, principles of restitution or unjust enrichment or otherwise for any loss, damages, cost or expense which may arise from or be incurred or suffered on account of anything contained in this e-tender or otherwise, including the accuracy, adequacy, correctness, completeness or reliability of the e-tender and any assessment, assumption, statement or information contained therein or deemed to form part of this e-tender or arising in any way with pre-qualification of

Bidders for participation in the Bidding Process. The Brihanmumbai Municipal Corporation (BMC) also accepts no liability of any nature whether resulting from negligence or otherwise caused arising from reliance of any Bidder.

Section II - Bid Data Sheet (BDS)

ITB Clause No.	Information	Details
	A. General	
3.	Number of members allowed in JV/Consortium/Sub-Contracting	Joint Venture or Consortium will NOT be allowed to participate in the bidding for the subject work.
	C. Preparation of Bids	
18.	Bid Validity Period	180-Calendar Days from the Date of Submission of Bid
	D. Submission and Opening of Bids	
25.	Date, time, and venue of opening of Pre-qualification and Technical covers received in response to the E-Procurement Notice	**19.06.2025 after 4 P.M.** Office of Director (IT), Basement, Annex Building, Municipal Head Office, 1, Mahapalika Marg, Fort, Mumbai – 400 001
25.	Date, time, and venue of technical presentations by qualified bidders	**To be informed.** Office of Director (IT), Basement, Annex Building, Municipal Head Office, 1, Mahapalika Marg, Fort, Mumbai – 400 001
25.	Date, time, and venue of opening of financial cover received in response to the E-Procurement Notice	**To be informed To be informed** Office of Director (IT), Basement, Annex Building, Municipal Head Office, 1, Mahapalika Marg, Fort, Mumbai – 400 001
	E. Award Criteria	
40.	Performance Security	10% of the contract value valid upto the entire contract period + 6 Months (including defect liability period.), within 30 days from the date of the award of the contract or prior to signing of the contract whichever is earlier or as intimated in the notification of intention to award/work order issued by BMC.

Section III - Evaluation and Qualification Criteria

BMC will evaluate and compare the Bids that have been determined to be substantially responsive, pursuant to ITB - Evaluation of Bids.

1. Evaluation of Prequalification

The prequalification bids shall be evaluated for submission and conformance of all documents with respect to prequalification criteria mentioned in this section.

Factor	**1. Eligibility**		
Sub-Factor	**Criteria**		**Documentation Required**
	Requirement	**Bidder**	
1.1 Registered Legal Entity	The following entities will be allowed to participate in the bid process: 1. Companies registered under the Indian Companies Act, 1956/2013 2. Partnership firms registered under the Limited Liability Partnerships (registered under LLP Act, 2008) 3. Partnership firms registered under the Indian Partnership Act, 1932	Must meet requirement	Form Bidder Information Form & Bidder's JV / Consortium Members Information Form (if applicable), with attachments of a Copy of Certificate of Incorporation signed by Authorized Signatory of the MSP/CSP, certified deed of partnership
1.2 Conflict of Interest	No- conflicts of interests as described in ITB - Eligible Bidders.	Must meet requirement	Letter of Bid
1 .3 BMC Ineligibility	Not having been declared ineligible by the BMC as described in ITB - Eligible Bidders.	Must meet requirement	Letter of Bid
1.4 Debarment	The MSP & CSP should not have been blacklisted by any Central/State Government Organization or Department in India at the time of submission of the bid.	Must meet requirement	Declaration by the MSP & CSP as per format given in the section – Bidding Forms
1.5 State owned Entity	Compliance with conditions of ITB – Eligible Bidders	Must meet requirement	Form – Bidder Information Form and Bidder's JV/Consortium Member Information Form (if applicable), with attachments
1.6 Power of Attorney in favour of lead bidder	Compliance with conditions of ITB - Documents Comprising the Bid	Must meet requirement	Power of Attorney
Factor	**2. Financial Situation**		
2.1 Historical Financial Performance	Submission of audited balance sheets, other financial statements acceptable to the BMC, for the last Three [3] years to demonstrate the current soundness of the Bidders financial position and its prospective long-term profitability. [Net worth is required to be positive]	Must meet requirement	Form – Historical Financial Performance, with attachments of Certificate from the Chartered Accountant clearly stating the net worth

2.2 Average Annual Turnover of bidder	Minimum average annual turnover calculated as total certified payments received for providing IT Services /Cloud Services/ Data Centre Services contracts in progress or completed, within the last three (3) years. **= 295 Crore or above**	Must meet requirement	Form – Average Annual Turnover from IT/Cloud Services projects, along with details of Extracts from the audited balance sheet and profit & loss; OR Certificate from the statutory auditor / Chartered Accountant
Factor	**3 Experience**		
3.1 General Experience	Experience under IT- Services Data Centre / Cloud Services contracts and/or implementing or Managing Vulnerability Management, Application Security and Cloud Posture Management in the role of prime Managed Service Provider, JV member, or subcontractor for at least the last three [3] years prior to the applications submission deadline..	Must meet requirement	Form – General Experience
3.2.1 Specific Experience	The MSP/CSP must have experience of successful migration and / or management of Cloud project(s) during last five years (as on the last date of bid submission) in Central / State Government/Urban Local Bodies / Public Sector Companies / Banking Financial Services & Insurance (BFSI)/ Private Sector of below mentioned project value in India: Project shall include setting up & hosting of IT infrastructure & systems at Cloud/ Private cloud or Infrastructure as a Service (IaaS) or Platform as a Service (PaaS) for contracts involving provisioning, testing, and operations & maintenance of Cloud Services 1. At least one project with a value not less than**48 Crore OR** 2. At least two projects with a value not less than**35 Crore OR** 3. At least three projects with a value not less than**24 Crore**	Must meet requirement	Form Specific Experience along with Completion certificates from the client; OR Work order + Self certificate of completion (Certified by the statutory auditor / Chartered Accountant); OR Work Order + Phase Completion Certificate from the client
Factor	**4 Certifications & Registrations**		
4.1 Certifications	MSP must have following certifications: - ISO 9001, ISO 27001, ISO/IEC 20000, CMMI Level 3 or more	Must meet requirement	Copy of the Valid Certificate signed and stamped by the Authorized Signatory of the Bidder.

4.2 GST and Income Tax Registration	Valid GST Registration and Income Tax Permanent Account Number (PAN)	Must meet requirement	Copy of GST registration number and PAN card
4.3 CSP Authorization	The MSP must be authorized by the proposed Cloud Service Provider and should be affiliated with the proposed CSP's cloud platform for at least Five years in India.	Must meet requirement	Copy of Authorization Letter
Factor	**5 Technical Manpower**		
5.1 Manpower	The MSP must have strength of at least 50 IT Professionals (data center/networking/system administration/cloud services / cloud security, maintenance of cloud solution/ virtual server administration/system administration, database etc) on their payroll as on date of submission of this bid. At least 10 of these professionals must have certification(s) in Cloud expertise areas.	Must meet requirement	Self-declaration from the Authorized signatory of the MSP on their letterhead
5.2	The MSP/ OEM's must have atleast 10 Certified Engineers in the proposed Vulnerability Management and Cloud Security tools	Must meet requirement	Copy of Certificates along with Self-declaration from the Authorized signatory of the MSP/OEM's on their letterhead
Factor	**6 Cloud Service Provider (CSP)**		
6.1 Empanelment	The CSP should be a MeitY Empaneled Cloud Service Provider (CSP) & STQC Audit Compliant.	Must meet requirement	Undertaking from the bidder on the letter head of the company, mentioning that CSP is a MeitY Empaneled and STQC Audit Compliant.
6.2 Certifications	CSP must have following certifications: - ISO 27001, ISO 27017, ISO 27018	Must meet requirement	Copy of the Valid Certificate signed and stamped by the Authorized Signatory of the CSP.
6.3 Accreditations	CSP should have accreditations. Relevant to security, availability, confidentiality, processing integrity, and/or privacy Trust Services principles. SOC 1, SOC 2, SOC 3 and PCI DSS	Must meet requirement	Self-declaration from the Authorized signatory of the CSP on their letterhead
Factor	**7 Cyber Security Tool**		
7.1 Experience	The proposed Vulnerability Tool must be hosted in a MeiTY approved Data Center	Must Meet Requirement	Undertaking from OEM to be submitted
7.2 Certifications	The proposed Cyber Security Tool should have following ISO Certification.	Must Meet Requirement	Copy of the valid Certificate signed and stamped by Authorized Signatory of the Bidder

	ISO/IEC 270001:2013 ISO/IEC 27017: 2015 ISO/IEC 27018: 2019 Trust and Compliance: 1. The Security, Trust, Assurance and Risk 2. Data Privacy Framework (DPF)		
Factors	**8. Original Equipment Manufacturer Certificate**		
8.1 MAF	The Bidder must provide OEM MAF for all the solutions provided.	Must Meet Requirement	Signed and stamped MAF by OEM to be provided

[1] For contracts under which the Bidder participated as a joint venture member or sub-contractor, only the Bidder's share, by value, and role and responsibilities shall be considered to meet this requirement.

In the case of a Bidder who offers to supply and install major items of supply under the contract that the Bidder did not manufacture or otherwise produce, the Bidder shall provide the manufacturer's authorization, using the form provided in Section – Bidding Forms, showing that the Bidder has been duly authorized by the manufacturer or producer of the related sub system or component to supply and install that item to BMC. The Bidder is responsible for ensuring that the manufacturer or producer complies with the requirements of ITB – Qualification of the Bidder and ITB – Sections of Bidding Document and meets the minimum criteria listed above for that item.

2. Technical Evaluation of the bids would be carried as follows:

#	Parameter	Evaluation Points	Max Marks	Documents required
1.	**Annual Turnover of bidder:** Minimum average annual turnover calculated as total certified payments received for providing Data Centre / Cloud Projects contracts in progress or completed, within the last three (3) years. = 295 Crore or above	Annual Turn over of bidder is 295-325 Cr = **15 marks** If bidder turnover is more than 325 Cr = **20 Marks**	20 Marks	Form – Average Annual Turnover from Cloud Services/ Data Center Services projects, along with details of Extracts from the audited balance sheet and profit & loss; OR Certificate from the statutory auditor / Chartered Accountant
3.	**General Experience** Experience under IT- Projects / Cloud projects / Data Centre contracts in the role of prime Managed Service Provider, JV member, or subcontractor for at least the last three [3] years prior to the applications submission deadline.	• 4 projects: **15 marks** • Additional 1 mark for each project more than 4 projects up to **20 marks**	20 marks	Form General Experience along with Completion certificates from the client; OR Work order + Self certificate of completion (Certified by the statutory auditor / Chartered Accountant); OR Work Order + Phase Completion Certificate from the client Bidder should also submit a certification from the client confirming the value of the project
4.	**Specific Experience** The Bidder must have experience of successful migration and / or management of Cloud project(s) during last five years (as on the last date of bid submission) in Central / State Government/Urban Local Bodies / Public Sector Companies / Banking Financial Services & Insurance (BFSI)/ Private Sector of below mentioned project value in India: Project shall include setting up & hosting of IT infrastructure & systems at Cloud/ Private cloud / Infrastructure as a Service (IaaS) or Platform as a Service (PaaS) for contracts involving provisioning, testing, and operations & maintenance of Cloud Services 1. At least one project with a value not less than 48 Crore **OR**	1. At least one project with a value not less than 48 Crore **OR** 2. At least two projects with a value not less than 35 Crore **OR** 3. At least three projects with a value not less than 24 Crore **Marks 15** **----------** **OR** 1. More than one project with a value not less than 48 Crore **OR**	20 marks	Form Specific Experience along with Completion certificates from the client; OR Work order + Self certificate of completion (Certified by the statutory auditor / Chartered Accountant); OR Work Order + Phase Completion Certificate from the client Bidder should also submit a certification from the client confirming the value of the project

	OR 2. At least two projects with a value not less than 35 Crore OR 3. At least three projects with a value not less than 24 Crore	2. More than two projects with a value not less than 35 Crore **OR** 3. More than three projects with a value than 24 Crore **Marks 20**		
5.	**Technical Manpower-** The MSP must have strength of at least 50 IT Professionals (data centre/networking/system administration/cloud services / cloud security, maintenance of cloud solution/ virtual server administration/system administration, database etc) on their payroll as on date of submission of this bid. At least 10 of these professionals must have certification(s) in Cloud expertise areas.	• 50 to 100 : **10 marks.** • More than 100 : **15 marks**.	15 Marks	Employees State Insurance Corporation (ESIC) / Provident Fund (PF) certificate should be submitted for IT professionals and certification of 10 IT professionals for proposed technical solution.
5.	**Empanelment:** The CSP should be a MeitY/ MahaIT/ DIT Empaneled Cloud Service Provider (CSP)	• Empanelled for more than 3 years: **15 Marks** • Empanelled for less than 3 years: **10 Marks**	15 Marks	Undertaking from the bidder on the letter head of the company, mentioning that CSP is a MeitY Empaneled and STQC Audit Compliant. And/or MeitY empaneled letter with validity.
7.	**Technical Presentation:** - Every bidder will be given a timeslot of 30 minutes to demonstrate the proposed Cloud Services implementation including design, configuration, operations and maintenance of applications on such platform.	Bidder should provide • Cloud architecture & design • Migration Plan • Security Measures & Compliance • Scalability & Performance • Additional services and value-added features	10 Marks	Technical proposal as a part of technical bid

3. Evaluation of Technical & Commercial Bid

1. The Technical Bids of only those Bidders, who qualify in the Pre-Qualification (and/or Technical Qualification) stage, shall be considered and will be evaluated as per the evaluation criteria in this clause. The Bid Evaluation Committee (BEC) shall invite each Bidder to make a presentation cum-demonstration as part of the technical evaluation.

2. The BEC may require written clarifications from the Bidders to clarify ambiguities and uncertainties arising out of the evaluation of the Bid documents (to be stated precisely as it should be in BMC's interest). For more details, please refer ITB - Clarification of Bids.
3. In order to qualify technically, a Bid must secure a minimum of 70% of total marks in technical evaluation after summing up. Only those Bids that have a minimum score of 70% of total marks in technical evaluation will be considered for opening of their Commercial Bid. Only the Bids qualifying the technical evaluation will be considered for commercial evaluation.
4. BMC reserves the right to lower the minimum required marks if none of the Bidders achieves 70% of the total marks.
5. Only the Bids qualifying the technical evaluation will be considered for commercial evaluation.
6. If the bidder is found non-responsive after evaluation of pre-qualification and technical documents, in such circumstances, the bidder will be made non-responsive and financial cover of non-responsive bidder will not be opened.

3. Technical Evaluation of the bids would be carried as follows:

1. BMC shall appoint a Bid Evaluation Committee (BEC) to scrutinize and evaluate the prequalification, technical and commercial bids received.
2. The BEC will examine the Bids to determine whether they are complete, responsive and whether the bid format conforms to the bid requirements. BMC may waive any informality or non-conformity in a bid which does not constitute a material deviation according to BMC.
3. The bid prices should not be mentioned in any part of the bid other than the Commercial Bid.
4. Any attempt by a bidder to influence the bid evaluation process may result in the rejection of Bid.
5. The Technical Bids of only those Bidders, who qualify & meet all the criteria in the Pre-Qualification stage, shall be considered, and will be evaluated as per the evaluation criteria given in the section below by the Bid Evaluation Committee (BEC).
6. The BEC may require written clarifications from the Bidders to clarify ambiguities and uncertainties arising out of the evaluation of the Bid.
4. Combined Evaluation (For Quality and Cost Based Selection – QCBS)

BEC will evaluate and compare the Bids that have been determined to be substantially responsive. An Evaluated Bid Score (B) will be calculated for each responsive Bid using the

following formula (for comparison in percentages), which permits a comprehensive assessment of the Bid price and the technical merits of each Bid:

$$B \equiv \frac{Clow}{C} * X * 100 + \frac{T}{Thigh} * (1 - X) * 100$$

Where,
C = Evaluated Bid Price
C low = the lowest of all Evaluated Bid Prices among responsive Bids
T = the total Technical Score awarded to the Bid
Thigh = the Technical Score achieved by the Bid that was scored best among all Responsive Bids
X = weight for the Cost as specified in the BDS
The Bid with the best evaluated Bid Score (B) among responsive Bids shall be the Most Advantageous Bid provided the Bidder was prequalified and/or it was found to be qualified to Perform the Contract.

Section IV- Bidding Forms

1. Letter of Bid

Date of this Bid submission: [*insert date (as day, month and year) of Bid submission*]

RFB No.: [*insert number of RFB process*]

To:

Department Office Address:

We, the undersigned, declare that:

(a) **No reservations:** We have examined and have no reservations to the bidding document, including Addenda/ Corrigendum issued in accordance with ITB - Sections of Bidding Document;

(b) **Eligibility**: We meet the eligibility requirements and have no conflict of interest in accordance with ITB – Eligible Bidders;

(c) **Bid-Securing Declaration:** We have not been suspended nor declared ineligible by the BMC / State Government / Central Government based on execution of a Bid-Securing Declaration or Proposal-Securing Declaration in India in accordance with ITB – Eligible Bidders;

(d) **Conformity:** We offer to provide the Services in conformity with the bidding document of the following: Selection of System Integrator for Implementation of services for BMC;

(e) **Bid Validity Period:** Our Bid shall be valid until *[insert day, month and year in accordance with ITB – Period of Validity of Bids],* and it shall remain binding upon us and may be accepted at any time before the expiration of that period;

(f) **Performance Security:** If our Bid is accepted, we commit to obtain a Performance Security in accordance with the bidding document;

(g) **One Bid Per Bidder:** We are not submitting any other Bid(s) as an individual Bidder, and we are not participating in any other Bid(s) as a Joint Venture member or as a subcontractor, and meet the requirements of ITB – Eligible Bidders, other than alternative Bids submitted in accordance with ITB – Alternative Bids;

(h) **Suspension and Debarment**: We, along with any of our subcontractors, Cloud Service Providers, consultants, manufacturers, or service providers for any part of the contract, are not subject to, and not controlled by any entity or individual that is subject to, a temporary suspension or a debarment imposed by the BMC. Further, we are not ineligible under the Indian laws;

(i) **State-owned enterprise or institution**: [*select the appropriate option and delete the other*] [*We are not a state-owned enterprise or institution*] / [*We are a state-owned enterprise or institution but meet the requirements of ITB - Eligible Bidders*];

(j) **Binding Contract**: We understand that this Bid, together with your written acceptance thereof included in your Letter of Acceptance, shall constitute a binding contract between us, until a formal contract is prepared and executed;

(k) **Not Bound to Accept:** We understand that you are not bound to accept the lowest evaluated cost Bid, the Most Advantageous Bid or any other Bid that you may receive; and

(l) **Fraud and Corruption:** We hereby certify that we have taken steps to ensure that no person acting for us or on our behalf engages in any type of Fraud and Corruption.

Name of the Bidder: *[*insert complete name of the Bidder*]

Name of the person duly authorized to sign the Bid on behalf of the Bidder: ** [*insert complete name of person duly authorized to sign the Bid*]

Title of the person signing the Bid: [*insert complete title of the person signing the Bid*]

Signature of the person named above: [*insert signature of person whose name and capacity are shown above*]

Date signed [*insert date of signing*] **day of** [*insert month*], [*insert year*]

*: In the case of the Bid submitted by a Joint Venture specify the name of the Joint Venture as Bidder.

**: Person signing the Bid shall have the power of attorney given by the Bidder. The power of attorney shall be attached with the Bid Schedules.

2. Bidder Information Form

[The Bidder shall fill in this Form in accordance with the instructions indicated below. No alterations to its format shall be permitted and no substitutions shall be accepted.]

Date: *[insert date (as day, month and year) of Bid submission*]

RFB No.: *[insert number of Bidding process]*

1. Bidder's Name *[insert Bidder's legal name]*
2. In case of JV, legal name of each member: *[insert legal name of each member in JV]*
3. Bidder's country of registration: *[insert country of registration]*
4. Bidder's year of registration: *[insert Bidder's year of registration]*
5. Bidder's Address in country of registration: *[insert Bidder's legal address in country of registration]*
6. Bidder's Authorized Representative Information Name: *[insert Authorized Representative's name]* Address: *[insert Authorized Representative's Address]* Telephone/Fax numbers: *[insert Authorized Representative's telephone/fax numbers]* Email Address: *[insert Authorized Representative's email address]*
7. Attached are [scanned] copies of original documents of *[check the box(es) of the attached original documents]* • Articles of Incorporation (or equivalent documents of constitution or association), and/or documents of registration of the legal entity named above, in accordance with ITB – Eligible Bidders. • In case of JV, letter of intent to form JV or JV agreement, in accordance with ITB – Eligible Bidders. • In case of state-owned enterprise or institution, in accordance with ITB – Eligible Bidders, documents establishing: o Legal and financial autonomy o Operation under commercial law o Establishing that the Bidder is not under the supervision of the agency of the BMC 8. Included are the list of Board of Directors and organizational chart

3. Bidder's JV / Consortium Members Information Form

[The Bidder shall fill in this Form in accordance with the instructions indicated below. The following table shall be filled in for the Bidder and for each member of a Joint Venture]].

Date: *[insert date (as day, month and year) of Bid submission*]
RFB No.: *[insert number of bidding process]*

1. Bidder's Name: *[insert Bidder's legal name]*
2. Bidder's JV / Consortium Member's name: *[insert JV's Member legal name]*
3. Bidder's JV / Consortium Member's country of registration: *[insert JV's Member country of registration]*
4. Bidder's JV / Consortium Member's year of registration: *[insert JV's Member year of registration]*
5. Bidder's JV / Consortium Member's legal address in country of registration: *[insert JV's Member legal address in country of registration]*
6. Bidder's JV / Consortium Member's authorized representative information Name: *[insert name of JV's Member authorized representative]* Address: *[insert address of JV's Member authorized representative]* Telephone/Fax numbers: *[insert telephone/fax numbers of JV's Member authorized representative]* Email Address: *[insert email address of JV's Member authorized representative]*
7. Attached are copies of original documents of *[check the box(es) of the attached original documents]* ¨ Articles of Incorporation (or equivalent documents of constitution or association), and/or registration documents of the legal entity named above, in accordance with ITB - Qualification of the Bidder. ¨ In case of a state-owned enterprise or institution, documents establishing legal and financial autonomy, operation in accordance with commercial law, and they are not under the supervision of BMC in accordance with ITB – Qualification of the Bidder. ¨ Included are the organizational chart, a list of Board of Directors, and the beneficial ownership.

4. Format for Declaration by the Bidder for not being Blacklisted / Debarred

(On Stamp Paper of Rs 500)
(To be submitted on the Letterhead of the responding firm)

DECLARATION CUM-INDEMNITY BOND

Date: dd/mm/yyyy

I,_____of _____,do hereby declared and undertake as under.

1) I declared that I have submitted certificates as required to Executive Engineer (Monitoring) at the time of registration of my firm / company _____ and there is no change in the contents of the certificates that are submitted at the time of registration.

2) I declared that I _____ in capacity as Manager / Director / Partners / Proprietors of _____ has not been charged with any prohibitory and /or penal action such as demotion, suspension, black listing / de-registration or any other action under the law by any Government and / or Semi Government and/ or Government Undertaking.

3) I declared that, I have perused and examined the tender document including addendum, condition of contract, specification, drawings, bill of quantity etc. forming part of tender and accordingly, I submit my offer to execute the work as per tender documents at the rates quoted by me in capacity as _____ of _____.

4) I further declared that if, I am allotted the work and I failed to carry out the allotted work in accordance with the terms and conditions and within the time prescribed and specified, BMC is entitled to carry out the work allotted to me by any other means at my risk and cost, at any stage of the contract.

5) I also declared that I will not claim any charge / damages / compensation for non availability of site for the contract work at any time.

6) I Indemnify Municipal Commissioner and the other officers of BMC or their agents for any Damages, Loss, or Injury, any legal suit, proceeding or legal action whatsoever that may be caused at any time by me or any other staff of_____ company, for the work undertaken and all such damage, damages, injury or loss, legal suit, legal action, I shall be solely responsible in individual as well as official capacity and such loss, damages, injury shall be made good and/ or as the case may be shall be paid immediately by me / Company to the satisfaction of the BMC.

Dated _____ day of _____, 20__

Identified by me

Before me

Advocate

5. Historical Financial Performance

Bidder's Legal Name: _____ Date: _____
JV Member Legal Name: _____RFB No.: _____

Page _____ of _____ pages

To be completed by the Bidder and, if JV, by each member

Financial information in INRequivalent	Historic information for previous _____ (__) years (INR equivalent in Lakhs)						
	Year 1	Year 2	Year 3	Year …	Year n	Avg.	Avg. Ratio
Information from Balance Sheet							
Total Assets (TA)							
Total Liabilities (TL)							
Net Worth (NW)							
Current Assets (CA)							
Current Liabilities (CL)							
Information from Income Statement							
Total Revenue (TR)							
Profits Before Taxes (PBT)							

Attached are copies of financial statements (balance sheets, including all related notes, and income statements) for the years required above complying with the following conditions:

a. Must reflect the financial situation of the Bidder or member to a JV, and not sister or parent companies
b. Historic financial statements must be audited by a certified accountant
c. Historic financial statements must be complete, including all notes to the financial statements
d. Historic financial statements must correspond to accounting periods already completed and audited (no statements for partial periods shall be requested or accepted)

6. Average Annual Turnover

Bidder's Legal Name: _____ Date: _____

JV Member Legal Name: _____ RFB No.: _____

Page _____ of _____ pages

Annual turnover data (applicable activities only)		
Year	Amount and Currency	INR equivalent
	_____	_____
	_____	_____
	_____	_____
	_____	_____
	_____	_____
*Average Annual Construction Turnover	_____	_____

*Average annual turnover calculated as total certified payments received for work in progress or completed, divided by the number of years specified in Section - Evaluation and Qualification Criteria.

7. Experience - General Experience

Bidder's Legal Name: _____ Date: _____

JV Member Legal Name: _____ RFB No.: _____

Starting Month / Year	Ending Month / Year	Years*	Contract Identification	Role of Bidder
_____	_____		Contract name: Brief Description of the Cloud Services performed by the Bidder: Name of Purchaser: Address:	_____

______	______		Contract name: Brief Description of the Cloud Services performed by the Bidder: Name of Purchaser: Address:	_________
______	______		Contract name: Brief Description of the Cloud Services performed by the Bidder: Name of Purchaser: Address:	_________
______	______		Contract name: Brief Description of the Cloud Services performed by the Bidder: Name of Purchaser: Address:	_________
______	______		Contract name: Brief Description of the Cloud Services performed by the Bidder: Name of Purchaser: Address:	_________
______	______		Contract name: Brief Description of the Cloud Services performed by the Bidder: Name of Purchaser: Address:	_________

8. Specific Experience

Bidder's Legal Name: ___________________________ Date: _____________________

JV Member Legal Name: _________________________ RFB No.: __________________

Relevant IT project experience	
General Information	
Name of the project	

Client for which the project was executed	
Name and contact details of the client	
Project Details	
Description of the project	
Scope of services	
Service levels being offered/ Quality of service (QOS)	
Technologies used	
Outcomes of the project	
Other Details	
Total cost of the project	
Total cost of the services provided by the respondent	
Duration of the project (no. of months, start date, completion date, current status)	
Other Relevant Information	
Letter from the client to indicate the successful completion of the projects	
Copy of Work Order	

9. Financial Proposal Template

Covering letter

To:

<Location, Date>

<Name>

<Designation>

<Address>

<Phone Nos.>

<Fax Nos.>

<Email id>

Subject: Submission of the Financial bid for <Provide Name of the Implementation Assignment>

Dear Sir/Madam,

We, the undersigned, offer to provide the Implementation services for <<Title of Implementation Services>> in accordance with your Request for Proposal dated <<Date>> and our Proposal (Technical and Financial Proposals). Our attached Financial Proposal is for the sum of <<Amount in words and figures>>. This amount is inclusive of the local taxes.

1. PRICE AND VALIDITY

- All the prices mentioned in our Tender are in accordance with the terms as specified in the RFB documents. All the prices and other terms and conditions of this Bid are valid for a period of **180** calendar days from the date of opening of the Bid.
- We hereby confirm that our prices include all taxes except GST. However, all the taxes are quoted separately under relevant sections.
- We understand that the actual payment would be made as per the existing tax rates during the time of payment.

2. UNIT RATES

- We have indicated in the relevant forms enclosed, the unit rates for the purpose of on account of payment as well as for price adjustment in case of any increase to / decrease from the scope of work under the contract.

3. TENDER PRICING

- We further confirm that the prices stated in our bid are in accordance with your Instruction to Bidders included in Tender documents.

4. QUALIFYING DATA

- We confirm having submitted the information as required by you in your Instruction to Bidders. In case you require any other further information/documentary proof in this regard before evaluation of our Tender, we agree to furnish the same in time to your satisfaction.

5. BID PRICE

- We declare that our Bid Price is for the entire scope of the work as specified in the Section – BMC's Requirements. These prices are indicated Commercial Bid attached with our Tender as part of the Tender.

6. PERFORMANCE BANK GUARANTEE

- We hereby declare that in case the contract is awarded .to us, we shall submit the Performance Bank Guarantee as specified in the <Appendix III> of this RFB document.

Our Financial Proposal shall be binding upon us subject to the modifications resulting from Contract negotiations, up to expiration of the validity period of the Proposal, i.e., [Date].

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

We hereby declare that our Tender is made in good faith, without collusion or fraud and the information contained in the Tender is true and correct to the best of our knowledge and belief.

We understand that our Tender is binding on us and that you are not bound to accept a Tender you receive.

Yours sincerely,

Authorized Signature:

Name and Title of Signatory: Name of Firm:

Address:

10. Personnel Capabilities

Name of Bidder or partner of a Joint Venture

1.	Title of position
	Name of prime candidate
2.	Title of position
	Name of prime candidate
3.	Title of position
	Name of prime candidate
4.	Title of position
	Name of prime candidate

11. Candidate Summary

Name of Bidder or partner of a Joint Venture

Position		Candidate ☐Prime☐Alternate
Candidate information	Name of candidate	Date of birth
	Professional qualifications	
Present employment	Name of Employer	
	Address of Employer	
	Telephone	Contact (manager / personnel officer)
	Fax	Telex
	Job title of candidate	Years with present Employer

Summarize professional experience over the last twenty years, in reverse chronological order. Indicate particular technical and managerial experience relevant to the project.

From	To	Company/Project/ Position/Relevant technical and managem experience

12. Manufacturer's Authorization form

Note: This authorization should be written on the letterhead of the Manufacturer and be signed by a person with the proper authority to sign documents that are binding on the Manufacturer.

Invitation for Bids Title and No.: [*Purchaser insert: **RFB Title and Number***]

To: [*Purchaser insert: **Purchaser's Officer to receive the Manufacture's Authorization***]

WHEREAS *[insert: **Name of Manufacturer**]* who are official producers of *[insert: **items of supply by Manufacturer**]* and having production facilities at *[insert: **address of Manufacturer**]* do hereby authorize *[insert: **name of Bidder or Joint Venture**]* located at *[insert: **address of Bidder or Joint Venture**]* (hereinafter, the "Bidder") to submit a bid and subsequently negotiate and sign a Contract with you for resale of the following Products produced by us:

We hereby confirm that, in case the bidding results in a Contract between you and the Bidder, the above-listed products will come with our full standard warranty.

Name *[insert: **Name of Officer**]* in the capacity of *[insert: **Title of Officer**]*

Signed _____

Duly authorized to sign the authorization for and on behalf of: *[insert: **Name of Manufacturer**]*

Dated this *[insert**ordinal**]* day of [*insert: **month***], *[insert: **year***].

[add Corporate Seal (where appropriate)]

13. Subcontractor's Agreement

Note: This agreement should be written on the letterhead of the Subcontractor and be signed by a person with the proper authority to sign documents that are binding on the Subcontractor.

Invitation for Bids Title and No.: [*Purchaser insert: **RFB Title and Number***]

To: [*Purchaser insert:* ***BMC's Officer to receive the Subcontractor's Agreement]***

WHEREAS *[insert:* ***Name of Subcontractor****],* having head offices at *[insert:* ***address of Subcontractor****],* have been informed by *[insert:* ***name of Bidder or Joint Venture****]* located at *[insert:* ***address of Bidder or Joint Venture*** *]* (hereinafter, the "Bidder") that it will submit a bid in which *[insert:* ***Name of Subcontractor*** *]* will provide *[insert:* ***items of supply or services provided by the Subcontractor*** *].* We hereby commit to provide the above-named items, in the instance that the Bidder is awarded the Contract.

Name *[insert:* ***Name of Officer****]* in the capacity of *[insert:* ***Title of Officer]***

Signed _____

Duly authorized to sign the authorization for and on behalf of: *[insert:* ***Name of Subcontractor****]*

Dated this *[insert:* ***ordinal*** *]* day of *[insert:* ***month*** *]*, *[insert:* ***year*** *]*.

[add Corporate Seal (where appropriate)]

14. List of Proposed Subcontractors

#	Item	Proposed Subcontractor	Place of Registration & Qualifications

15. Technical Capabilities

Name of Bidder or partner of a Joint Venture

The Bidder shall provide adequate information to demonstrate clearly that it has the technical capability to meet the requirements for the Cloud Services. With this form, the Bidder should summarize important certifications, proprietary methodologies, and/or specialized technologies that the Bidder proposes to utilize in the execution of the Contract or Contracts.

16. Format of the Technical Bid

In accordance with ITB – Documents Establishing Conformity of Services, the documentary evidence of conformity of the Cloud Services to the bidding documents includes (but is not restricted to):

a. The Bidder's Preliminary Project Plan, including, but not restricted, to the topics specified in the BDS ITB – Documents Establishing Conformity of Services. The Preliminary Project Plan should also state the Bidder's assessment of the major responsibilities of BMC and any other involved third parties in System supply and installation, as well as the Bidder's proposed means for coordinating activities by each of the involved parties to avoid delays or interference.

b. A written confirmation by the Bidder that, if awarded the Contract, it shall accept responsibility for successful integration and interoperability of all the proposed Information Technologies included in the System, as further specified in the Technical Requirements.

c. Item-by-Item Commentary on the Technical Requirements demonstrating the substantial responsiveness of the overall design of the System and the individual Information Technologies, Goods, and Services offered to those Technical Requirements in the following format.

Technical Responsiveness Checklist

Sr. No.	Technical Requirement Details	Compliance Yes / No / Clarification if any
B	Functional, Architectural, Performance & Security Requirements	
1	Legal and Regulatory Requirements to be met by the Cloud Services	
1.1	Data Protection and Privacy Laws:	
	Comply with applicable data protection and privacy laws if any.	Yes
	Implement appropriate security measures to protect personal and sensitive information stored in the Cloud Services.	Yes
	Obtain necessary consent from individuals for the collection, storage, and processing of their personal data.	Yes
1.2	....	
1.3	...	

In demonstrating the responsiveness of its bid, the Bidder must use the Technical Responsiveness Checklist (Format as given above). Failure to do so significantly increases the risk that the Bidder's Technical Bid will be declared technically non-responsive. Among other

things, the checklist should contain explicit cross-references to the relevant pages in supporting materials included the Bidder's Technical Bid.

Note:The Technical Requirements are voiced as requirements of the Cloud Service Provider and/or the System. The Bidder's response must provide clear evidence for the evaluation team to assess the credibility of the response. A response of "yes" or "will do" is unlikely to convey the credibility of the response. The Bidder should indicate that – and to the greatest extent practical – how the Bidder would comply with the requirements if awarded the contract. Whenever the technical requirements relate to feature(s) of existing products (e.g., hardware or software), the features should be described, and the relevant product literature referenced. When the technical requirements relate to professional services (e.g., analysis, configuration, integration, training, etc.) some effort should be expended to describe how they would be rendered – not just a commitment to perform the [cut-and-paste] requirement. Whenever a technical requirement is for the Cloud Service Provider to provide certifications (e.g., ISO 9001), copies of these certifications must be included in the Technical Bid.

d. Supporting materials to underpin the Item-by-item Commentary on the Technical Requirements (e.g., product literature, white-papers, narrative descriptions of technical approaches to be employed, etc.). In the interest of timely bid evaluation and contract award, Bidders are encouraged not to overload the supporting materials with documents that do not directly address BMC's requirements.

e. Any separate and enforceable contract(s) for Recurrent Cost items which the Bidder is required to bid.

Note: To facilitate bid evaluation and contract award, Bidders encouraged to provide electronic copies of their Technical Bid – preferably in a format that the evaluation team can extract text from to facilitate the bid clarification process and to facilitate the preparation of the Bid Evaluation Report.

17. Intellectual Property Forms

Notes to Bidders on working with the Intellectual Property Forms

In accordance with ITB 11.1(j), Bidders must submit, as part of their bids, lists of all the Software included in the bid assigned to one of the following categories: (A) System, General-Purpose, or Application Software; or (B) Standard or Custom Software. Bidders must also submit a list of all Custom Materials. These categorizations are needed to support the Intellectual Property in the GCC.

18. Software List

	(Select one per item)			(Select one per item)	
Software Item	System Software	General-Purpose Software	Application Software	Standard Software	Custom Software

19. List of Custom Materials

Custom Materials

20. Authorization letter for attending pre-bid meeting / bid opening

(To be provided on the letter head of Bidder)

No……..… Date……

To

The……

Brihanmumbai Municipal Corporation,

Mumbai.

Subject: - Attending Pre-bid Meeting / Bid Opening

Reference: - Bid No…….…… due date…….

Sir,

We here by authorize Mr./Ms. …….as our authorized representative, to represent us on the following occasion: -

- Pre-bid Meeting to be held on……..at…….A.M./P.M.
- Bid Opening on…… At…… A.M. /P.M.

Kindly permit him/her to attend the same.

Yours faithfully,

Signature:

Name of signatory:

Designation:

Rubber Stamp:

21. Pre-Bid Query Format

Bidder requiring specific points of clarification may communicate with Information Technology Department during the specified period using the following format:

BIDDER 'S REQUEST FOR CLARIFICATION	
<<Name of Organization submitting query / request for clarification>>	
<<Full formal address of the Organization including phone, fax and email points of contact>>	Tel: Fax: Email:

Sr No.	Page No.	Section No.	Point No.	Existing Clause	Clarification/Query of Bidder

Please prepare the above table in Excel Format as shown above. Any other format shall not be entertained.

22. Table of Legal, Stationery Charges, Stamp Duty, and List of Approved Banks for Submission of Performance Security

Table of Legal & Stationery Charges

Contract Value	Legal Charges + Stationery Charges
Up to Rs. 50,000/-	Not Applicable
Rs. 50,001/- to Rs. 1,00,00,000/-	0.10% of the contract value (In the multiple of 100/-) + 18% GST Minimum Rs.1000/- + applicable GST and Max. Rs.10.000/- +applicable GST
Rs.1,00,00,001/- to Rs.10,00,00,000/-	Rs.10,000/- for the initial Rs.1,00,00,000/- + for the remaining contract value above Rs.1,00,00,000/- shall be 0.05% (In the multiple of 100/-) + 18% applicable GST
Above Rs. 10,00,00,001 /-	Rs. 55,000/- for first Rs.10 crore + 0.01% of remaining contract amount +18% GST

In case of revision of the above mentioned legal and stationary charges, bidder shall pay revised legal and stationary charges.

Stamp Duty Charges Payable By Successful Bidder

#	Where the amount or value set forth in such contract does not exceed rupees five lakh.	Five Hundred rupees stamp duty
1	Where it exceeds rupees five lakhs	Five hundred rupees plus 0.3% of the amount above rupees five lakh subject to the maximum of rupees twenty-five lakh stamp duty.
2	Stamp Duty on Bank Guarantee	0.3% for the amount secured by Bank Guarantee subject to maximum of rupees twenty lakh.

a. The successful Bidder shall enter into a contract agreement with BMC within 30 days from the date of issue of LOA/Work Order and the same should be adjudicated for payment of Stamp Duty by the successful Bidder.

b. Further shortfall if any, in amount of stamp duty paid as against prescribed amount for the documents executed in Mumbai City and Mumbai Suburban District be recovered from the concerned work contractors and to deposit the deficit or unpaid Stamp Duty and penalty by two separate Demand Draft or Pay Order in favors of “Superintendent of Stamp, Mumbai” within 15 days from intimation thereof.

c. All legal charges and incidental expenses in this respect shall be borne and paid by the successful Bidder(s).

List of Approved Banks

The Performance Security (Bank Guarantee) issued by branches of approved Banks beyond Kalyan and Virar can be accepted only if the said Bank Guarantee is countersigned by the Manager of a Branch of

the same Bank within the Mumbai City limit categorically endorsing thereon that the said Bank Guarantee is binding on the endorsing Branch of the Bank within Mumbai limits and is liable to be enforced against the said Branch of the Bank in case of default by the Managed / Cloud Service Provider furnishing the Banker's guarantee.

Nationalized Banks.		
Bank of Baroda	Bank of India	Bank of Maharashtra
Canara Bank	Central Bank of India	Indian Bank
Indian Overseas Bank	Punjab & Sind Bank	Punjab National Bank
State Bank of India	UCO Bank	Union Bank of India
Private Sector Banks.		
Axis Bank Ltd.	Bandhan Bank Ltd.	CSB Bank Ltd.
City Union Bank Ltd.	DCB Bank Ltd.	Dhanlaxmi Bank Ltd.
Federal Bank Ltd.	HDFC Bank Ltd	ICICI Bank Ltd.
Induslnd Bank Ltd	IDFC First Bank Ltd.	Jammu & Kashmir Bank Ltd.
Karnataka Bank Ltd.	Karur Vysya Bank Ltd.	Kotak Mahindra Bank Ltd
Lakshmi Vilas Bank Ltd.	Nainital Bank Ltd.	RBL Bank Ltd.
South Indian Bank Ltd.	Tamilnad Mercantile Bank Ltd.	YES Bank Ltd.
IDBI Bank Ltd.		
Scheduled Urban Co-op. Banks Licensed to issued Bankers Guarantee.		
Abhyudaya Co-Op. Bank Ltd.	Bassein Catholic Co-Op. Bank Ltd.	Bharat Co-Op. Bank Ltd.
Bombay Mercantile Co-Op. Bank Ltd.	Citizen Credit Co-Op. Bank Ltd.	DombivliNagariSahakari Bank Ltd.
Greater Mumbai Co-Op. Bank Ltd.	Janakalyan Sahakari Bank Ltd.	Janata Sahakari Bank Ltd.
Kalyan Janata Sahakari Bank Ltd.	Kapol Co-Op. Bank Ltd.	Mahanagar Co-Op. Bank Ltd.
Mumbai District Central Co-Op. Bank Ltd.	NKGSB Co-Op. Bank Ltd.	New India Co-Op. Bank Ltd.
Parsik Janata Sahakari Bank Ltd.	Punjab & Maharashtra Co-Op. Bank Ltd.	Rupee Co-Op. Bank Ltd.
Sangli Urban Co-Op. Bank Ltd.	Saraswat Co-Op. Bank Ltd.	Thane Bharat Sahakari Bank Ltd.
Thane Janata Sahakri Bank Ltd.	The Cosmos Co-Op. Bank Ltd.	The ShamraoVitthal Co-Op. Bank Ltd.
The Zoroastrian Co-Op. Bank.		
State Co-op. Banks.		
The Maharashtra State Co-Op. Bank.		
Foreign Banks.		
Australia and New Zealand Banking Group Ltd.	Westpac Banking Corporation	Bank of Bahrain & Kuwait BSC
AB Bank Ltd.	Sonali Bank Ltd.	Bank of Nova Scotia
Industrial & Commercial Bank of China Ltd.	BNP Paribas	Credit Agricole Corporate & Investment Bank
Societe Generale	Deutsche Bank	HSBC Ltd
PT Bank Maybank Indonesia TBK	Mizuho Bank Ltd.	Sumitomo Mitsui Banking Corporation
The Bank of Tokyo- Mitsubishi UFJ, Ltd.	CooperatieveRabobank U.A.	Doha Bank
Qatar National Bank	JSC VTB Bank	Sberbank
United Overseas Bank Ltd	Bank of China Ltd.	Shinhan Bank
Woori Bank	KEB Hana Bank	Industrial Bank of Korea
Kookmin Bank	Bank of Ceylon	Credit Suisse A.G

CTBC Bank Co., Ltd.	Krung Thai Bank Public Co. Ltd.	Abu Dhabi Commercial Bank Ltd.
Mashreq Bank PSC	First Abu Dhabi Bank PJSC	Emirates Bank NBD
Barclays Bank Plc.	Standard Chartered Bank	NatWest Markets Plc
American Express Banking Corporation	Bank of America	Citibank N.A.
J.P. Morgan Chase Bank N.A.	SBM Bank (India) Limited*	DBS Bank India Limited*

23. CONTRACT FORMS

Notes to the BMC on preparing the Contract Forms

Performance Security: Pursuant to GCC Clause - Securities, the successful Bidder is required to provide the Performance Security within thirty (30) days of notification of Contract award.

Advance Payment Security: Pursuant to Clause Securities, the successful Bidder is required to provide a bank guarantee securing the Advance Payment, if the GCC Clause – Terms of Payment provides for an Advance Payment.

Installation and Operational Acceptance Certificates: Recommended formats for these certificates are included in this RFB. Unless the BMC has good reason to require procedures that differ from those recommended, or to require different wording in the certificates, the procedures and forms shall be included unchanged. If the BMC wishes to amend the recommended procedures and/or certificates, it may propose alternatives for the approval of the World Bank before release of the bidding document to potential Bidders.

Change Order Procedures and Forms: Similar to the Installation and Operational Acceptance Certificates, the Change Estimate Proposal, Estimate Acceptance, Change Proposal, Change Order, and related Forms should be included in the bidding document unaltered. If the BMC wishes to amend the recommended procedures and/or certificates, it may propose alternatives for the approval of the World Bank before release of the bidding document.

Notes to Bidders on working with the Sample Contractual Forms

The following forms are to be completed and submitted by the successful Bidder following notification of award: (i) Contract Agreement, with all Appendices; (ii) Performance Security; and (iii) Advance Payment Security.

- Contract Agreement: In addition to specifying the parties and the Contract Price, the Contract Agreement is where the: (i) Cloud Service Provider's Representative; (ii) if applicable, agreed Adjudicator and his/her compensation; and (iii) the List of Approved Subcontractors are specified. In addition, modifications to the successful Bidder's Bid Price Schedules are attached to the Agreement. These contain corrections and adjustments to the Cloud Service Provider's bid prices to correct errors, adjust the Contract Price to reflect – if applicable - any extensions to bid validity beyond the last day of original bid validity plus 56 days, etc.
- Performance Security: Pursuant to GCC Clause Securities, the successful Bidder is required to provide the Performance Security in the form contained in this section of these bidding documents and in the amount specified in accordance with the BDS.
- Advance Payment Security: Pursuant to GCC Clause - Securities, the successful Bidder is required to provide a bank guarantee for the full amount of the Advance Payment - if an Advance Payment is specified in the for GCC Clause Terms of Payment - in the form contained in this section of these bidding documents or another form acceptable to the BMC. If a Bidder wishes to propose a different Advance Payment Security

form, it should submit a copy to the BMC promptly for review and confirmation of acceptability before the bid submission deadline.

The BMC and Managed / Cloud Service Provider will use the following additional forms during Contract implementation to formalize or certify important Contract events: (i) the Installation and Operational Acceptance Certificates; and (ii) the various Change Order forms. These and the procedures for their use during performance of the Contract are included in the bidding documents for the information of Bidders.

1. CONTRACT AGREEMENT

Request For Bids No…… Due on …/…/..…

Sanction No. …… Dated……

Contract for Carrying out work of .....……...……

During the period from …… to ……..

Contract Cost:……

THIS AGREEMENT MADE ON THIS ……. Day of …… Two Thousand …… Between…… (Partner /Proprietor's Full Name) in habitant/s of Mumbai, carrying on business at …… in Mumbai under the style and name of Messrs …… for and on behalf of himself / themselves, his / their heirs, executors, administrators and assigns (Hereinafter called "the Contractor/s") of the FIRST PART and ……..……..…….. Shri/ Smt. ..... the Director/Dy. Municipal Commissioner in which expressions are included unless such inclusion is inconsistent with the context or meaning therefore include Director/Dy. Municipal Commissioner and any officers of Brihanmumbai Municipal Corporation authorized by the Director/Dy. Municipal Commissioner and shall also include their successors & assign / assignee for the time being holding office, of the SECOND PART and the Brihanmumbai Municipal Corporation (Hereinafter called "the Corporation") of the THIRD PART.

WHEREAS the Municipal Commissioner for Greater Mumbai has inter alia deputed under Section 56 and 56 (b) of the Mumbai Municipal Corporation Act 1888 his powers, functions and duties under the provisions contained in Chapter III of the Mumbai Municipal Corporation Act 1888 to the Director/Dy. Municipal Commissioner

AND WHEREAS the Director/Dy. Municipal Commissioner in pursuance of the power vested in him / her under the provision of the Mumbai Municipal Corporation Act 1888 and in accordance with the provision of the said Act, invited bid for the work of……. and / or certain work mentioned in the schedule / specification here to annexed.

AND WHEREAS the contractor/s has/have submitted bid for the said work and his / their said bid was accepted by the Municipal Commissioner with the approval of the Mayor/ Standing Committee/ Education Committee of the Corporation on the Terms and Conditions hereinafter specified.

AND WHEREAS the said Contractor/s has / have paid deposit of ₹……./- (Rupees……) in the office of …….. as Performance Security for the due and faithful performance of this contract OR has / have furnished the General Undertaking and Guarantee for ₹……./- (Rupees…… ……) of Bank, for the payment interallia of the said amount of the Contract Deposit in the office of …….. for the due and faithful performance of this contract.

NOW THESE PRESENTS WITNESS and it is hereby agreed and declared between and by the parties hereto as follows:-

In this agreement words and expressions shall have the same meanings as are respectively assigned to them in the General Conditions of Contract for works hereinafter referred to.

NOW IT IS HEREBY AGREED as follows:

Article 1. Contract Documents

1.1 Contract Documents (Reference GCC Clause (Definitions))

The following documents shall constitute the Contract between the BMC and the Cloud Service Provider, and each shall be read and construed as an integral part of the Contract:

(a) This Contract Agreement and the Appendices attached to the Contract Agreement
(b) Special Conditions of Contract
(c) General Conditions of Contract
(d) Technical Requirements (including Implementation Schedule)
(e) The Cloud Service Provider's bid and original Price Schedules
(f) ***[Add here: any other documents]***

1.2 Order of Precedence (Reference GCC Clause (Contract Documents))

In the event of any ambiguity or conflict between the Contrac Documents listed above, the order of precedence shall be the orde in which the Contract Documents are listed in Article 1.1 (Contrac Documents) above, provided that Appendix 7 shall prevail over al provisions of the Contract Agreement and the other Appendices attached to the Contract Agreement and all the other Contrac Documents listed in Article 1.1 above.

1.3 Definitions (Reference GCC Clause (Definitions))

Capitalized words and phrases used in this Contract Agreemen shall have the same meanings as are ascribed to them in the General Conditions of Contract.

Article 2. Contract Price and Terms of Payment

2.1 Contract Price (Reference GCC Clause (Definitions) and GCC Clause (Contract Price))

The BMC hereby agrees to pay to the Managed / Cloud Service Provider the Contract Price in consideration of the performance by the Managed / Cloud Service Provider of its obligations under the Contract. The Contract Price shall be the aggregate of: ***[insert: amount in words],[insert: amount in figures],*** as specified in the Price Schedule.

The Contract Price shall be understood to reflect the terms and conditions used in the specification of prices in the detailed price

schedules, including the terms and conditions of the associated Incoterms, and the taxes, duties and related levies if and as identified.

Article 3. Effective Date for Determining Time for Operational Acceptance

3.1 Effective Date (Reference GCC Clause (Definitions))

The time allowed for supply, installation, and achieving Operational Acceptance of the System shall be determined from the date when all of the following conditions have been fulfilled:

(a) This Contract Agreement has been duly executed for and on behalf of the BMC and the Cloud Service Provider;

(b) The Managed / Cloud Service Provider has submitted to the BMC the performance security and the advance payment security, in accordance with GCC Clause (Securities);

Each party shall use its best efforts to fulfill the above conditions for which it is responsible as soon as practicable.

3.2 If the conditions listed under 3.1 are not fulfilled within two (2) months from the date of this Contract Agreement because of reasons not attributable to the Cloud Service Provider, the parties shall discuss and agree on an equitable adjustment to the Time for Achieving Operational Acceptance and/or other relevant conditions of the Contract.

Article 4. Appendixes

4.1 The Appendixes listed below shall be deemed to form an integral part of this Contract Agreement.

4.2 Reference in the Contract to any Appendix shall mean the Appendixes listed below and attached to this Contract Agreement, and the Contract shall be read and construed accordingly.

APPENDIXES

Appendix 1. Cloud Service Provider's Representative
Appendix 2. Adjudicator *[if there is no Adjudicator, state **"not applicable"**]*
Appendix 3. List of Approved Subcontractors
Appendix 4. Categories of Software
Appendix 5. Custom Materials
Appendix 6. Revised Price Schedules (if any)
Appendix 7. Minutes of Contract Finalization Discussions and Agreed-to Contract Amendments

In consideration of the payments to be made by the Commissioner to the contractor as hereinafter mentioned the contractor hereby covenants with the Commissioner to complete the Works / Supply in all respects with the provision of the contract.

The Commissioner hereby covenants to pay to the Contractor in consideration of the completion of the works/ supply the contract sum, at times and in the manner prescribed by the contract.

IN WITNESS WHERE of the parties hereto have caused their respective common seals to be hereto affixed (or hereunto set their respective hands and seals) the day and year above written.

Signed, Sealed and delivered

By ……..…..

Of ……..……

In the presence of Contractors

1) ……..……

2) ……..

Signed, Sealed and delivered

By ……..…..

in the presence of Director/ Dy. MC

1) ……..……

2) ……..……

The Common seal of the Municipal Corporation of

Brihanmumbai was affixed on this ……. Day of

….…… 20….. in the presence of

(1) ……..……

(2) ....……..…… SEAL

two Members of the Standing Committee

of the Brihanmumbai Municipal Corporation

and in the presence of the Municipal Secretary.

……

Municipal Secretary

APPENDIX 1. CLOUD SERVICE PROVIDER'S REPRESENTATIVE

In accordance with GCC Clause (Definitions), the Cloud Service Provider's Representative is:

Name: ***[insert: name and provide title and address further below, or state "to be nominated within fourteen (14) days of the Effective Date"]***

Title: ***[if appropriate, insert: title]***

In accordance with GCC Clause (Notices), the Cloud Service Provider's addresses for notices under the Contract are:

Address of the Cloud Service Provider's Representative: ***[as appropriate, insert: personal delivery, postal, cable, telegraph, telex, facsimile, electronic mail, and/or EDI addresses.]***

Fallback address of the Cloud Service Provider: ***[as appropriate, insert: personal delivery, postal, cable, telegraph, telex, facsimile, electronic mail, and/or EDI addresses.]***

APPENDIX 2. ADJUDICATOR

In accordance with GCC Clause (Definitions) and GCC Clause (Settlement of Disputes), the agreed-upon Adjudicator is:

Name: ***[insert: name]***

Title: ***[insert: title]***

Address: ***[insert: postal address]***

Telephone: ***[insert: telephone]***

APPENDIX 3. LIST OF APPROVED SUBCONTRACTORS

The BMC has approved use of the following Subcontractors nominated by the Managed / Cloud Service Provider for carrying out the item or component of the System indicated. Where more than one Subcontractor is listed, the Managed / Cloud Service Provider is free to choose between them, but it must notify the BMC of its choice sufficiently in advance of the time when the subcontracted work needs to commence to give the BMC reasonable time for review. In accordance with GCC Clause (Subcontracting), the Managed / Cloud Service Provider is free to submit proposals for Subcontractors for additional items from time to time. No subcontracts shall be placed with any such Subcontractors for additional items until the Subcontractors have been approved in writing by the BMC and their names have been added to this list of Approved Subcontractors, subject to GCC Clause (Subcontracting).

[specify: item, approved Subcontractors, and their place of registration that the Managed / Cloud Service Provider proposed in the corresponding attachment to its bid and that the BMC approves that the Managed / Cloud Service Provider engage during the performance of the Contract. Add additional pages as necessary.]

Item	Approved Subcontractors	Place of Registration

APPENDIX 4. CATEGORIES OF SOFTWARE

The following table assigns each item of Software supplied and installed under the Contract to one of the three categories: (i) System Software, (ii) General-Purpose Software, or (iii) Application Software; and to one of the two categories: (i) Standard Software or (ii) Custom Software.

	(select one per item)			(select one per item)	
Software Item	System Software	General-Purpose Software	Application Software	Standard Software	Custom Software

APPENDIX 5. CUSTOM MATERIALS

The follow table specifies the Custom Materials the Managed / Cloud Service Provider will provide under the Contract.

Custom Materials

APPENDIX 6. REVISED PRICE SCHEDULES

The attached Revised Price Schedules (if any) shall form part of this Contract Agreement and, where differences exist, shall supersede the Price Schedules contained in the Cloud Service Provider's Bid. These Revised Price Schedules reflect any corrections or adjustments to the Cloud Service Provider's bid price.

APPENDIX 7. MINUTES OF CONTRACT FINALIZATION DISCUSSIONS AND AGREED-TO CONTRACT AMENDMENTS

The attached Contract amendments (if any) shall form part of this Contract Agreement and, where differences exist, shall supersede the relevant clauses in the GCC, Technical Requirements, or other parts of this Contract as defined in GCC Clause (Contract Documents).

2. DRAFT NON-DISCLOSURE AGREEMENT

(TobesubmittedonaRs.500Stamp Paper)

This Non-Disclosure Agreement ("Non-Disc") is made and entered into dayof month year (effective date)

By and between _____("BMC")and __("Cloud Service Provider").

Whereas,BMCandManaged / Cloud Service Provider haveenteredintoanAgreement("Agreement")

effective _____;and for

Whereas, each party desires to disclose to the other party certain information in oral or

writtenform,whichisproprietaryandconfidentialtothedisclosingparty,("CONFIDENTIALINFORMATION").

NOW,THEREFORE, in consideration of the foregoing and the covenants and agreements contained herein, the parties agree as follows:

1. **Definitions.** As used herein:
   a) Theterm "Confidential Information "shall include, without limitation, all information and materials, furnished byeitherPartytotheotherinconnectionwithcitizen/users/persons/customers data, products and/or services, including information transmitted in writing, orally, visually, (e.g. video terminal display) or on magnetic or optical media, and including all proprietary information, customer and prospect lists, trade secrets, trade names or proposed trade names, methods and procedures of operation, commercial or marketing plans, licensed document know-how, ideas, concepts, designs, drawings, flowcharts, diagrams, quality manuals, checklists, guidelines, processes, formulae, source code materials, specifications, programs, software packages, codes and other intellectual property relating to the disclosing party's data, computer database, products and/or services. Results of any tests, sample surveys, analytics, datamining exercises or usages etc. carried out by the receiving party in connection with theBMC'sinformationincludingcitizen/users/persons/customersperso

nalor sensitive personal information as defined under any law for the time being in force shall also be considered Confidential Information.

b) Theterm,"BMC"shallincludetheofficers,employees,agents,consultants, contractors and representatives of BMC.

c) Theterm, "Cloud Service Provider "shall include the directors, officers, employees, agents, consultants, contractors and representatives of Cloud Service Provider, including its applicable affiliates and subsidiary companies.

2. **ProtectionofConfidentialInformation:**WithrespecttoanyConfidentialInformationdisclosedtoitortowhich ithasaccess, Managed / Cloud Service Provider affirms that it shall:

a) Use the Confidential Information as necessary only in connection with Project and in accordance with the terms and conditions contained herein;

b) Maintain the Confidential Information in strict confidence and take all reasonable stepstoenforcetheconfidentialityobligationsimposedhereunder,butinnoeventtakelesscarewith the Confidential Information that the parties take to protect the confidentiality of its own proprietary and confidential information and that of its clients;

c) Not to make or retain copy of any commercial or marketing plans, citizen/users/persons/customers database, Bids developed by or originating from BMC or any of the prospective clients of BMC except as necessary, under prior written intimation from BMC, in connection with the Project, and ensure that any such copy is immediately returned to BMC even without express demand from BMC to do so;

d) Not disclose or in any way assist or permit the disclosure of any Confidential Information to any other person or entity without the express written consent of the other party; and

e) Return to the other party, or destroy, at BMC's discretion, any and all Confidential Information disclosed in a printed form or other permanent record, or in any other tangible form (including without limitation, all copies, notes, extracts, analyses, studies, summaries, records and reproductions thereof) immediately upon the earlier to occur of

(i) Expiration or termination of either party's engagement in the Project, or(ii)the request

Of the other party therefore.

f) Not to discuss with any member of public, media, press, any or any other person about the nature of arrangement entered between BMC and Managed / Cloud Service Provider or the nature of services to be provided by the Managed / Cloud Service Provider to the BMC.

3. **Onus.** Managed / Cloud Service Provider shall have the burden of proving that any disclosure or use inconsistent with the terms and conditions hereof alls within any of the foregoing exceptions.

4. **Exceptions.** These restrictions as enumerated in section – "Protection of Confidential Information" of this Agreement shall not apply to any Confidential Information:

a) Which is independently developed by Managed / Cloud Service Provider or lawfully received from another source free of restriction and without breach of this Agreement; or

b) After it has become generally available to the public without breach of this Agreement by Cloud Service Provider; or

c) Which at the time of disclosure to Managed / Cloud Service Provider was known to such party free of restriction

And evidenced by documentation in such party's possession; or

d) Which BMC agrees in writing is free of such restrictions.

e) Which is received from a third party not subject to the obligation of confidentiality with respect to such Information;

5. **Remedies.** Managed / Cloud Service Provider acknowledges

that(a)any actual or threatened disclosure or use of the Confidential Information by Managed / Cloud Service Provider would be a breach of this agreement and may cause immediate and irreparable harm to BMC;(b)Managed / Cloud Service Provider affirms that damages from such disclosure or use by it may be impossible to measure accurately; and (c) injury sustained by BMC may be impossible to calculate and remedy fully. Therefore, Managed / Cloud Service Provider acknowledges that in the event of such a breach, BMC shall been titled to specific performance by Managed / Cloud Service Provider of Cloud Service Provider's obligations contained in this Agreement. In addition, Managed / Cloud Service Provider shall indemnify BMC of the actual and liquidated damages which may be demanded by BMC. Moreover, BMC shall be entitled to recover all costs (including reasonable attorneys' fees) which it or they may incur in connection with defending its interests and enforcement of legal rights arising due to a breach of this agreement by Cloud Service Provider.

6. **Need to Know.** Managed / Cloud Service Provider shallrestrictdisclosureofsuchConfidentialInformationtoitsemployees and/or consultants with a need to know (and advise such employees of the obligations assumed herein), shall use the Confidential Information only for the purposes set forth in the Agreement, and shall not disclose such Confidential Information to any affiliates, subsidiaries, associates and/ or third party without prior written approval of the disclosing party.

7. **Intellectual Property Rights Protection.** No license to a party, under any trademark, patent, copyright, design right, mask work protection right, or any other intellectual property right is either granted or implied by the conveying of Confidential Information to such party.

8. **No Conflict.** The parties represent and warrant that the performance of its obligations hereunder do not and shall not conflict with any other

agreement or obligation of the respective parties to which they are a party or by which the respective parties are bound.

9. **Authority.** The parties represent and warrant that they have all necessary authority and power to enter in to this Agreement and perform their obligations hereunder.

10. **Dispute Resolution.** If any difference or dispute arises between the BMC and the Managed / Cloud Service Provider in connection with the validity, interpretation, implementation or alleged breach of any provision of this Agreement, any such dispute shall be referred to the Hon. Municipal Commissioner, BMC before arbitration.

    a) The arbitration proceedings shall be conducted in accordance with the (Indian)ArbitrationandConciliationAct,1996andamendments thereof.

    b) The place of arbitration shall be Mumbai.

    c) The arbitrator's award shall be substantiated in writing and binding on the parties.

    d) The proceedings of arbitration shall be conducted in English language.

    e) The arbitration proceedings shall be completed within a period of 180 days from the date of reference of the dispute to arbitration.

11. **Governing Law.** This Agreement shall be interpreted in accordance with and governed by the substantive and procedural laws of India and the parties hereby consent to the exclusive jurisdiction of Courts and/or Forums situated at Mumbai, India only.

12. **EntireAgreement.**ThisAgreementconstitutestheentireunderstandingan dagreement of the parties, and supersedes all previous or contemporaneous agreement or communications, both oral and written, representations and under standings among the parties with respect to the subject matter hereof.

13. **Amendments.** No amendment, modification and/or discharge of this Agreement shall be valid or binding on the parties unless made in writing and signed on behalf of each of the parties by the irrespective duly authorized officers or representatives.

14. **Binding Agreement.** This Agreement shall be binding upon and inure to the benefit of the parties hereto and their respective successors and permitted as signs.

15. **Severability.** It is the intent of the parties that in case any one or more of the provisions contained in this Agreement shall be held to be invalid or unenforceable in any respect, such provision shall be modified to the extent necessary to render it, as modified, valid and enforceable under applicable laws, and such invalidity or unenforceability shall not affect the other provisions of this Agreement.

16. **Waiver.** If either party should waive any breach of any provision of this Agreement, its hall not thereby be deemed to have waived any preceding or succeeding breach of the same or any other provision hereof.

17. **Survival.** Both parties agree that all of their obligations undertaken herein with respect to Confidential Information received pursuant to this Agreement shall survive till perpetuity even after any expiration or termination of this Agreement.

18. **Non-solicitation.** During the term of this Agreement and there after for a further period of two (2) years Managed / Cloud Service Provider shall not solicit or attempt to solicit BMC's employees and /or consultants, for the purpose of hiring/ contractor to proceed to conduct operations/business similar to BMC with any employee and/or consultant of the BMC who has knowledge of the Confidential Information, without the prior written consent of BMC. This section will survive irrespective of the fact whether there exists a commercial

relationship between Managed / Cloud Service Provider and BMC.

19. **Term.** Subject to aforesaid section - Survival, this Agreement shall remain valid up to ….. years from the “effective date”.

INWITNESSHEREOF, and intending to be legally bound, the parties have executed this Agreement to make it effective from the date and year first written above.

For BMC

Name:

Title

WITNESSES:

1:

2:

For Cloud Service Provider

Name:

Title:

WITNESSES:

1:

2:

3. PERFORMANCE AND ADVANCE PAYMENT SECURITY FORMS

1.1 PERFORMANCE SECURITY FORM (BANK GUARANTEE)

[The bank, as requested by the successful Bidder, shall fill in this form in accordance with the instructions indicated]

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

(With Stamp duty of 03 % on the total amount)

Ref. No. :

Date :

Bank Guarantee No. :

To

<Insert complete postal address>

THIS INDENTURE made this ---------- day of ---------20---- BETWEEN THE ----------(Name of the Bank and address) BANK incorporated under the English / Indian Companies Acts and carrying on business in Mumbai (hereinafter referred to as 'the bank' which expression shall be deemed to include its successors and assigns) of the first part –---------- (Name of the Cloud Service Provider)

Inhabitants carrying on business at ---------- (Cloud Service Provider's Address)

in Mumbai under the style and name of Messers ----------(Name of the Cloud Service Provider)

(Hereinafter referred to as 'the contractors') of the second part Shri----------(Name of Municipal Commissioner)

THE MUNICIPAL COMMISSIONER FOR GREATER MUMBAI (hereinafter referred to as 'the Commissioner' which expression shall be deemed, also to include his successor or successors for the time being in the said office of Municipal Commissioner) of the third part and THE BRIHANMUMBAI MUNICIPAL CORPORATION (hereinafter referred to as 'the Corporation') of the fourth part WHEREAS the contractors indemnify and keep indemnified the Corporation against any loss or damage that may be caused to or suffered by the Corporation by reason of any breach by the contractors of any of the terms and conditions of the contract that will be entered subsequently (within 15 days) and/or in the performance thereof against Letter of Intent number ---------- dated ---------- for the project Selection of System Integrator for Implementation of services for BMC of ---------- department having tender No. <<>> tender amount Rs.---------- and the terms of such tender / contract require that the contractors shall deposit with the Commissioner as bid security and/ or the security a sum of Rs.---------- (Rupees----------) AND WHEREAS if and when any such tender is accepted by the Commissioner, the contract to be entered into in furtherance thereof by the contractors will provide that such deposit shall remain with and be appropriated by the Commissioner towards the security-deposit to be taken under the contract and be redeemable by the contractors, if they shall duly and faithfully carry out the terms and provisions of such contract and shall duly satisfy all claims properly chargeable against them there under AND WHEREAS the contractors are constituents of the Bank and in order to facilitate the keeping of the accounts of the contractors, the Bank with the consent and concurrence of the contractors has requested the Commissioner to accept the undertaking of the Bank hereinafter contained, in place of the contractors depositing with the Commissioner the said sum as bid security and/or the security as aforesaid AND WHEREAS accordingly the Commissioner has agreed to accept such undertaking. NOW THIS AGREEMENT WITNESSES that in consideration of the premises, the Bank at the request of the contractors (hereby testified) UNDERTAKES WITH the Commissioner to pay to the Commissioner upon demand in writing, whenever required by him, from time to time, so to do, a sum not exceeding in the whole Rs.----------(Rupees----------) under the terms of the said tender and/or the contract.

The B.G. is valid up to----------

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

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

IN WITNESS WHEREOF

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

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

Address ----------

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

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

Address ----------

----

the Bank and the said Messrs----------
----------(Name of the bank)

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

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

Address ----------

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

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

Address ----------

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

1.2 ADVANCE PAYMENT SECURITY

Bank Guarantee

_____

[Guarantor letterhead or SWIFT identifier code]

Beneficiary: *[insert: **Name and Address of BMC**]*
Date: ***[insert date of issue**]*
ADVANCE PAYMENT GUARANTEE No.: *[insert: **Advance Payment Guarantee Number**]*
Guarantor: *[Insert name and address of place of issue, unless indicated in the letterhead]*
We have been informed that on *[insert: **date of award**]* you awarded Contract No. *[insert: **Contract number**]* for *[insert: **title and/or brief description of the Contract**]* (hereinafter called "the Contract") to *[insert: **complete name of Cloud Service Provider, which in the case of a joint venture shall be the name of the joint venture**]* (hereinafter called "the Applicant").
Furthermore, we understand that, according to the conditions of the Contract, an advance payment in the sum of ***[insert: amount in numbers and words, for each currency of the advance payment]*** is to be made to the Managed / Cloud Service Provider against an advance payment guarantee.
At the request of the Applicant, we as Guarantor, hereby irrevocably undertake to pay the Beneficiary any sum or sums not exceeding in total an amount of *[insert amount in figures]*
(_____) *[insert amount in words]*[30] upon receipt by us of the Beneficiary's complying demand supported by the Beneficiary's statement, whether in the demand itself or in a separate signed document accompanying or identifying the demand, stating either that the Applicant:

a. has used the advance payment for purposes other than toward delivery of Goods; or
b. has failed to repay the advance payment in accordance with the Contract conditions, specifying the amount which the Applicant has failed to repay.

A demand under this guarantee may be presented as from the presentation to the Guarantor of a certificate from the Beneficiary's bank stating that the advance payment referred to above has been credited to the Applicant on its account number *[insert number]* at *[insert name and address of Applicant's bank]*.
The maximum amount of this guarantee shall be progressively reduced by the amount of the advance payment repaid by the Applicant as specified in copies of interim statements or payment certificates which shall be presented to us. This guarantee shall expire, at the latest, upon our receipt of a copy of the interim payment certificate indicating that ninety () percent of the Accepted Contract Amount, has been certified for payment, or on the *[insert day]* day of *[insert month]*, 2 *[insert year]*, whichever is earlier. Consequently, any demand for payment under this guarantee must be received by us at this office on or before that date.

_____
[signature(s)]

Note: All italicized text (including footnotes) is for use in preparing this form and shall be deleted from the final product.

2. LETTER OF ACCEPTANCE

[letterhead paper of the BMC]

[date]

To: *[name and address of the Service Provider]*

This is to notify you that your Bid dated *[date]* for execution of the *[name of the Contract and identification number, as given in the Special Conditions of Contract]* for the Contract Price of the equivalent of *[amount in numbers and words] [name of currency]*, as corrected and modified in accordance with the Instructions to Bidders is hereby accepted by BMC.

You are requested to furnish (i) the Performance Security within 30 days in accordance with the Conditions of Contract, using for that purpose one of the Performance Security Form*s*, included in Section –Bidding Forms, of the bidding document.

Authorized Signature: _____

Name and Title of Signatory: _____

Name of Organization: Information Technology Department, Brihanmumbai Municipal Corporation

Attachment: Contract

5. INSTALLATION AND ACCEPTANCE CERTIFICATES

5.1 INSTALLATION AND ACCEPTANCE CERTIFICATES

5.1Installation Certificate

Date:***[insert: date]***

RFB:***[insert: title and number of RFB]***
Contract:***[insert: name and number of Contract]***

To: ***[insert: name and address of Cloud Service Provider]***
Dear Sir or Madam:

Pursuant to GCC Clause (Installation of the System) of the Contract entered into between yourselves and the ***[insert: name of Purchaser]***(hereinafter the "BMC") dated ***[insert: date of Contract],*** relating to the ***[insert: brief description of the Cloud Services],*** we hereby notify you that the System (or a Subsystem or major component thereof) was deemed to have been correctly installed on the date specified below.

1.Description of the System (or relevant Subsystem or major component: ***[insert: description]***
2.Date of Installation: ***[insert: date]***

Notwithstanding the above, you are required to complete the outstanding items listed in the attachment to this certificate as soon as practicable. This letter shall not relieve you of your obligation to achieve Operational Acceptance of the System in accordance with the Contract nor of your obligations during the Warranty Period.

For and on behalf of the BMC

Signed:
Date:
in the capacity of: ***[state: "Project Manager" or state the title of a higher level authority in the BMC's organization]***

5.2 OPERATIONAL ACCEPTANCE CERTIFICATE

Date:***[insert: date]***
RFB:***[insert: title and number of RFB]***
Contract:***[insert: name of System or Subsystem and number of Contract]***

To: ***[insert: name and address of Cloud Service Provider]***

Dear Sir or Madam:

Pursuant to GCC Clause (Commissioning and Operational Acceptance) of the Contract entered into between yourselves and the ***[insert: name of Purchaser]*** (hereinafter the "BMC") dated ***[insert: date of Contract],*** relating to the ***[insert: brief description of the Cloud Services],*** we hereby notify you the System (or the Subsystem or major component identified below) successfully completed the Operational Acceptance Tests specified in the Contract. In accordance with the terms of the Contract, the BMC hereby takes over the System (or the Subsystem or major

component identified below), together with the responsibility for care and custody and the risk of loss thereof on the date mentioned below.
1.Description of the System (or Subsystem or major component): ***[insert: description]***
2.Date of Operational Acceptance: ***[insert: date]***

This letter shall not relieve you of your remaining performance obligations under the Contract nor of your obligations during the Warranty Period.

For and on behalf of the BMC

Signed:
Date:
in the capacity of: ***[state: "Project Manager" or higher level authority in the BMC's organization]***

6. CHANGE ORDER PROCEDURES AND FORMS

Date:***[insert: date]***
RFB:***[insert: title and number of RFB]***
Contract:***[insert: name or System or Subsystem and number of Contract]***

General

This section provides samples of procedures and forms for carrying out changes to the System during the performance of the Contract in accordance with GCC Clause (Changes to the System) of the Contract.

Change Order Log

The Managed / Cloud Service Provider shall keep an up-to-date Change Order Log to show the current status of Requests for Change and Change Orders authorized or pending. Changes shall be entered regularly in the Change Order Log to ensure that the log is kept up-to-date. The Managed / Cloud Service Provider shall attach a copy of the current Change Order Log in the monthly progress report to be submitted to the BMC.

References to Changes

(1)Request for Change Proposals (including Application for Change Proposals) shall be serially numbered CR-nnn.
(2)Change Estimate Proposals shall be numbered CN-nnn.
(3)Estimate Acceptances shall be numbered CA-nnn.
(4)Change Proposals shall be numbered CP-nnn.
(5)Change Orders shall be numbered CO-nnn.
On all forms, the numbering shall be determined by the original CR-nnn.

Annexes

6.1Request for Change Proposal Form
6.2Change Estimate Proposal Form
6.3Estimate Acceptance Form
6.4Change Proposal Form
6.5Change Order Form

6.6Application for Change Proposal Form

6.1Request for Change Proposal Form

(BMC's Letterhead)

Date:***[insert: date]***
RFB:***[insert: title and number of RFB]***
Contract:***[insert: name of System or Subsystem or number of Contract]***

To: ***[insert: name of Managed / Cloud Service Provider and address]***
Attention: ***[insert: name and title]***

Dear Sir or Madam:

With reference to the above-referenced Contract, you are requested to prepare and submit a Change Proposal for the Change noted below in accordance with the following instructions within ***[insert: number]*** days of the date of this letter.

1.Title of Change: ***[insert: title]***

2.Request for Change No./Rev.: ***[insert: number]***

3.Originator of Change: ***[select BMC / Managed / Cloud Service Provider (by Application for Change Proposal), and add: name of originator]***

4.Brief Description of Change: ***[insert: description]***

5.System (or Subsystem or major component affected by requested Change): ***[insert: description]***

6.Technical documents and/or drawings for the request of Change:

Document or Drawing No.Description

7.Detailed conditions or special requirements of the requested Change: ***[insert: description]***

8.Procedures to be followed:

(a)Your Change Proposal will have to show what effect the requested Change will have on the Contract Price.

(b)Your Change Proposal shall explain the time it will take to complete the requested Change and the impact, if any, it will have on the date when Operational Acceptance of the entire System agreed in the Contract.

(c)If you believe implementation of the requested Change will have a negative impact on the quality, operability, or integrity of the System, please provide a

detailed explanation, including other approaches that might achieve the same impact as the requested Change.

(d)You should also indicate what impact the Change will have on the number and mix of staff needed by the Managed / Cloud Service Provider to perform the Contract.

(e)You shall not proceed with the execution of work related to the requested Change until we have accepted and confirmed the impact it will have on the Contract Price and the Implementation Schedule in writing.

9.As next step, please respond using the Change Estimate Proposal form, indicating the proposed approach for implementing the Change, all its elements, and will also address the points in paragraph 8 above pursuant to GCC Clause (Changes to the System). Your Change Estimate Proposal should contain a first approximation of the proposed approach, and implications for schedule and cost, of the Change.

For and on behalf of the BMC

Signed:
Date:
in the capacity of: ***[state: "Project Manager" or higher level authority in the BMC's organization]***

6.2Change Proposal Form

(Cloud Service Provider's Letterhead)

Date:***[insert: date]***

RFB:***[insert: title and number of RFB]***
Contract:***[insert: name of System or Subsystem and number of Contract]***

To: ***[insert: name of Purchaser and address]***

Attention: ***[insert: name and title]***

Dear Sir or Madam:

In response to your Request for Change Proposal No. ***[insert: number],***we hereby submit our proposal as follows:

1.Title of Change: ***[insert: name]***

2.Change Proposal No./Rev.: ***[insert: proposal number/revision]***

3.Originator of Change: ***[select: BMC / Cloud Service Provider; and add: name]***

4.Brief Description of Change: ***[insert: description]***

5.Reasons for Change: ***[insert: reason]***

6.The System Subsystem, major component, or equipment that will be affected by the requested Change: ***[insert: description]***

7.Technical documents and/or drawings for the requested Change:
Document or Drawing No.Description

8.Estimate of the increase/decrease to the Contract Price resulting from the proposed Change: ***[insert: amount in currencies of Contract],*** as detailed below in the breakdown of prices, rates, and quantities.
Total lump sum cost of the Change:
Cost to prepare this Change Proposal (i.e., the amount payable if the Change is not accepted, limited as provided by GCC Clause 39.2.6):

9.Additional Time for Achieving Operational Acceptance required due to the Change: ***[insert: amount in days / weeks]***

10.Effect on the Functional Guarantees: ***[insert: description]***

11.Effect on the other terms and conditions of the Contract: ***[insert: description]***

12.Validity of this Proposal: for a period of ***[insert: number]*** days after receipt of this Proposal by the BMC

13.Procedures to be followed:
(a)You are requested to notify us of your acceptance, comments, or rejection of this detailed Change Proposal within ***[insert: number]*** days from your receipt of this Proposal.
(b)The amount of any increase and/or decrease shall be taken into account in the adjustment of the Contract Price.

For and on behalf of the Managed / Cloud Service Provider

Signed:
Date:
in the capacity of: ***[state: "Cloud Service Provider's Representative" or other higher level authority in the Cloud Service Provider's organization]***

6.3Change Order Form

(BMC's Letterhead)

Date:***[insert: date]***

RFB:***[insert: title and number of RFB]***

Contract:***[insert: name of System or Subsystem and number of Contract]***

To: ***[insert: name of Managed / Cloud Service Provider and address]***

Attention: ***[insert: name and title]***

Dear Sir or Madam:

We hereby approve the Change Order for the work specified in Change Proposal No. ***[insert: number]***, and agree to adjust the Contract Price, Time for Completion, and/or other conditions of the Contract in accordance with GCC Clause 39 of the Contract.

1.Title of Change: ***[insert: name]***

2.Request for Change No./Rev.: ***[insert: request number / revision]***

3.Change Order No./Rev.: ***[insert: order number / revision]***

4.Originator of Change: ***[select: BMC / Cloud Service Provider; and add: name]***

5.Authorized Price for the Change:
Ref. No.: ***[insert: number]***Date: ***[insert: date]***

[insert: amount in foreign currency A] plus ***[insert: amount in foreign currency B]*** plus ***[insert: amount in foreign currency C]*** plus ***[insert: amount in local currency]***

6.Adjustment of Time for Achieving Operational Acceptance: ***[insert: amount and description of adjustment]***

7.Other effects, if any: ***[state: "none" or insert description]***

For and on behalf of the BMC
Signed:
Date:
in the capacity of: ***[state: "Project Manager" or higher level authority in the BMC's organization]***

For and on behalf of the Managed / Cloud Service Provider

Signed:
Date:
in the capacity of: ***[state "Cloud Service Provider's Representative" or higher level authority in the Cloud Service Provider's organization]***

6.4Application for Change Proposal Form

(Cloud Service Provider's Letterhead)

Date:***[insert: date]***

RFB:***[insert: title and number of RFB]***
Contract:***[insert: name of System or Subsystem and number of Contract]***

To: ***[insert: name of Purchaser and address]***

Attention: ***[insert: name and title]***

Dear Sir or Madam:

We hereby propose that the below-mentioned work be treated as a Change to the System.

1.Title of Change: ***[insert: name]***

2.Application for Change Proposal No./Rev.: ***[insert: number / revision]*** dated: ***[insert: date]***

3.Brief Description of Change: ***[insert: description]***

4.Reasons for Change: ***[insert: description]***

5.Order of Magnitude Estimation: ***[insert: amount in currencies of the Contract]***

6.Schedule Impact of Change: ***[insert: description]***

7.Effect on Functional Guarantees, if any: ***[insert: description]***

8.Appendix: ***[insert: titles (if any); otherwise state "none"]***

For and on behalf of the Managed / Cloud Service Provider

Signed:
Date:
in the capacity of: ***[state: "Cloud Service Provider's Representative" or higher level authority in the Cloud Service Provider's organization]***

Part II – BMC's Requirements

Section V – BMC's Requirements

(INCLUDING TECHNICAL REQUIREMENTS, IMPLEMENTATION SCHEDULE, SYSTEM INVENTORY TABLES, BACKGROUND, AND INFORMATIONAL MATERIALS)

A. Background and Informational Materials

A.1 BACKGROUND

0.1 The BMC

0.1.1 Brihanmumbai Municipal Corporation (BMC) is a Local Self Government, governed by M.M.C. Act 1888 and providing various services to Citizens of Mumbai including health services, building permissions, water supply, sanitation, roads, storm water drains and many other services.

0.1.2 Information Technology Department of BMC is responsible for providing IT services in the city of Mumbai, hereafter may be referred to as IT Department of BMC.

0.1.3 Director (IT)heads Information Technology Department of BMCand is a decision-making authority with respect to proposed Cloud Services Contract. IT Department of BMC is the technical guidance agency to assist various BMC departments in driving the Information System project/s.

0.2 The BMC's Business Objectives for the Cloud Services

0.2.1 The primary objective of proposed Cloud Services is to manage and improve IT operations, efficiency, and security of BMC software applications.

0.2.2 Following is a breakdown of some key objectives a Cloud Service Provider (CSP) / Managed Service Provider (MSP) can help BMC achieve:

1. Enhanced IT Efficiency and Performance:

- **Reduced IT burden:** The CSP/ MSP handles day-to-day IT management tasks, freeing up BMC's internal IT staff to focus on strategic initiatives.
- **Standardized processes:** Standardized procedures ensure consistent and reliable IT service delivery.
- **Proactive maintenance:** The CSP / MSP proactively monitors and maintains BMC's IT infrastructure to prevent problems before they occur.
- **Improved uptime and performance:** By proactively addressing potential issues, the CSP / MSP helps minimize downtime and optimize IT system performance.

2. Increased Cost-Effectiveness:

- **Predictable IT costs:**CSP / MSP offers subscription-based pricing, providing predictable IT expenses and potentially reducing overall IT costs compared to maintaining an in-house IT team.
- **Access to expertise:**BMC gains access to a pool of skilled IT professionals without the overhead costs of hiring and training a full-time IT staff.

- **Reduced capital expenditure:** The CSP / MSP managesBMC's IT infrastructure, minimizing the need for upfront hardware and software investments.

3. Improved Security Posture:

- **Enhanced security measures:** The CSP / MSP implements and maintains robust security solutions, including firewalls, intrusion detection systems, and data encryption, to protect BMC's IT infrastructure from cyber threats.
- **Regular security updates and patching:** The CSP / MSP ensures BMC's systems are updated with the latest security patches to address vulnerabilities promptly.
- **Compliance with regulations:** The CSP / MSPis required to help BMC comply with relevant industry data security and privacy regulations.

4. Increased Business Continuity and Disaster Recovery:

- **Data backup and disaster recovery plans:** The CSP / MSP implements a robust data backup strategy and disaster recovery plan to ensure business continuity in case of outages or disruptions.
- **Disaster recovery testing and validation:** The CSP/ MSP regularly tests and validates BMC's disaster recovery plan to ensure its effectiveness.
- **Reduced downtime:** By having a well-defined disaster recovery plan, the CSP / MSP can help minimize downtime and get BMC's business back up and running quickly in case of an incident.

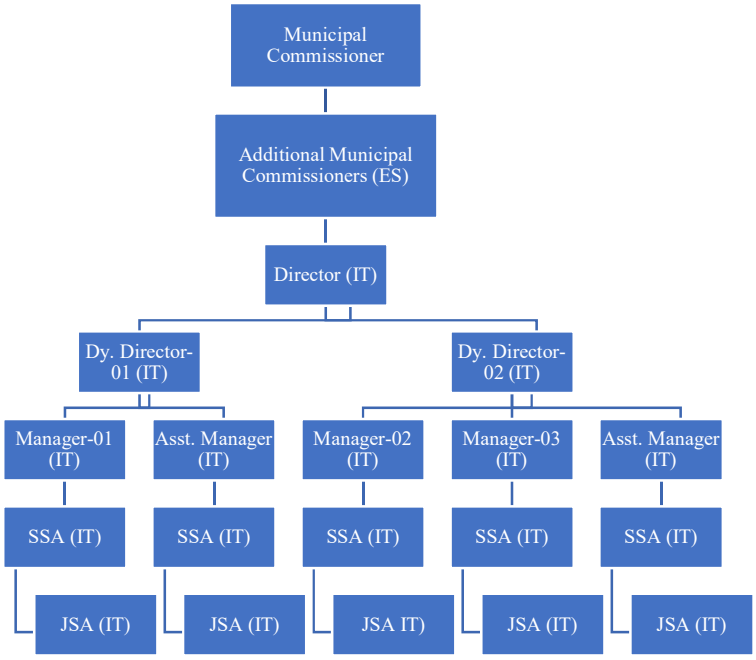
5. Improved User Experience:

- **Reliable and responsive IT support:** The CSP / MSP provides efficient help desk and support services to address user IT issues promptly, minimizing disruption to their productivity.
- **Access to latest technologies:** The CSP / MSP gives access to the latest IT solutions and technologies, allowing BMC users to work more efficiently and effectively.
- **Improved user training and education:** The CSP / MSP offers user training programs to help employees understand how to utilize IT systems effectively and securely.
- **Scalability and Flexibility:** The CSP's / MSP's services should be scalable to accommodate BMC's growth and evolving IT needs.
- **Improved Communication and Collaboration:** The CSP/ MSP should foster open communication and collaboration with BMC's internal IT team to ensure a smooth working relationship.

By partnering with an CSP/ MSP and leveraging it's expertise, BMC can achieve a range of objectives that contribute to a more efficient, secure, and cost-effective IT environment that supports the overall delivery of IT services.

0.4 Key Statistics of BMC DIT

0.4.1 Organization chart of department



0.4.2 Number of employees / users of proposed system – 25000+ employees

0.4.3 Number of offices with addresses – BMC has approximately 48 departments and 24 ward offices spread. across approximately 200 locations in Mumbai and Thane District (Water Supply Department)

0.4.4 Number of desktop PCs / printers / end devices etc. currently available in department – BMC has 350000+ users and approximately 20000+ PCs connected to its Worli Data Centre on its network.

0.4.5 Connectivity available with offices / locations – Abovementioned 200 Locations are connected to Worli Data

Centre through SDWAN and Point to Point connectivity. Worli Data Centre is connected to the Cloud Services on which BMC's applications are deployed.

A.2 INFORMATIONAL MATERIALS

0.1 Existing Cloud Services / Information Technologies Relevant to the Cloud Services

BMC at present has deployed following applications on Cloud Infrastructure provided by M/s. ESDS Software Solution Ltd. a MEITY empaneled Cloud Service Provider.

1. Building Permission System (AutoDCR)
2. Geographical Information System (GIS)
3. MyBMC Building UID
4. RETMS (Removal of Encroachment Tracking Management System)

Cloud resources consumed for the above BMC applications are listed below: -

The Cloud Service Provider is required to offer a comprehensive technical solution as per the requirements specified in this bid document that is compatible to function in tandem with the above-mentionedapplications / infrastructure items.

0.2 Stakeholders Roles and Responsibilities

Implementing an information software involves various stakeholders who play specific roles and have distinct responsibilities throughout the process. A clear definition of the roles and responsibilities of all the stakeholders in a project establishes transparency, accountability, manageability, and efficiency in the project. Following are the key stakeholders and their roles and responsibilities in implementing Cloud Services:

1. Executive Leadership: Executive leaders, Senior Administration of BMC, have the overall responsibility for driving the implementation of the information software. Their roles include:
    - Setting strategic objectives and goals for the implementation.
    - Allocating necessary resources, including budget and personnel.
    - Providing guidance and support to the implementation team.
    - Overseeing the progress and ensuring alignment with organizational priorities.
2. IT Department & Other Departments of BMC: IT managers and department heads of BMC are responsible for managing the technical aspects of the implementation. Their roles include:
    - Assessing the BMC's IT infrastructure and evaluating the compatibility and integration requirements of the information software.
    - Collaborating with other departments and stakeholders to ensure smooth integration and minimize disruptions.
3. End Users: End users, such as employees or citizens, contractors (providing various services to BMC and requiring transacting on BMC applications) play a crucial role in the successful adoption and utilization of the information software. Their responsibilities include:
    - Participating in user acceptance testing and providing feedback on the usability and functionality of the software platform.
    - Participating in training programs or workshops to acquire the necessary skills and knowledge to effectively use the software platform.
    - Adhering to security protocols, best practices, and organizational policies while using the software platform.
    - Providing ongoing feedback and suggestions for improvement to enhance the user experience.
4. Consultants: In some cases, BMC may engage consultants to assist with the implementation of the Cloud Services. Their responsibilities include:
    - Providing expertise, guidance, and support in the selection, installation, and configuration of the software platform.
    - Assisting with customization, integration, and migration tasks.
5. The Service Provider – The overall scope of work as well as roles & responsibilities for the selected Service Provider shall include but not limited to the services covering Installation, Testing, Commissioning, Operations, Maintenanceand Configuration of software applications for BMC as detailed in this bid document. The Service Provider's teams will have following roles and responsibilities:
    a. Project Manager: The project manager oversees the entire implementation process, ensuring effective coordination and timely completion of tasks. Their responsibilities include:
        - Developing a detailed project plan, including milestones, deliverables, and dependencies.
        - Planning and coordinating the implementation project, including resource allocation, timelines, and risk management.
        - Assigning tasks and responsibilities to team members, and tracking progress.
        - Managing risks, issues, and changes throughout the implementation.
        - Facilitating communication and collaboration among stakeholders.
        - Reporting project status, including successes, challenges, and recommendations, to executive leadership.
        - Overseeing the technical team and ensuring adherence to best practices and security standards.

b. Technical Team: The technical team, including developers, system administrators, and IT staff, plays a crucial role in implementing the Cloud Services. Their responsibilities include:
   - Installing, configuring, and customizing the Cloud Services based on the BMC's requirements.
   - Integrating the software platform with existing systems, databases, or third-party applications.
   - Testing and debugging the implementation to ensure functionality, performance, and security.
   - Providing ongoing maintenance, updates, and support for the software platform.
   - Offering training programs or workshops for end users.

c. Legal and Compliance Team: The legal and compliance team of BMC and the Cloud Service Provider ensures that the implementation of the Cloud Services adheres to relevant laws, regulations, and licensing requirements. Their responsibilities include:
   - Assessing the licensing terms and conditions of the Cloud Services and ensuring compliance with applicable licenses.
   - Reviewing and approving any modifications or customizations to ensure compliance with licensing obligations.
   - Evaluating data privacy and security considerations associated with the software platform.
   - Providing guidance on intellectual property rights and legal implications of using Cloud Services.

These stakeholders collaborate and coordinate their efforts to ensure a successful implementation of the Cloud Services. Clear communication, well-defined roles and responsibilities, and effective project management are essential for a smooth implementation process and the achievement of desired outcomes.

B. Scope of Work

BMC seeks to select single MSP to provide Cloud services for the contract duration mentioned in this RFP.

1. Provisioning, Configuring, Testing, Commissioning, Operating and Maintaining the Cloud Services

The scope of services shall comprise the following as summarized below:

- Study of the existing setup
- Project Planning and Management
- Design, provisioning, installation, configuration, and management of the Cloud DC & DR as per BMC's requirement
- Appropriate provisioning of technical/ skilled manpower
- Provide Internet Connectivity and Public IP
- Migration of the existing setup on the proposed Cloud environment
- Disaster Recovery (DR) planning, implementation, and DR Drills
- Cloud Security Solutions
- Testing
- Operations and Maintenance
- Training, Support and Documentation
- Security Solutions and VA/PT Audits.
- Backup and Restore Solution
- Monitoring and Reporting Services
- Helpdesk Services

In implementing the above, the bidder shall strictly adhere to the standards set by MeitY and

BMC. The proposed solution should be in line with MeitY guidelines. The details about the above-mentioned services are covered in subsequent sections.

2. Cloud Services

Provisioning of a reliable Cloud services from Ministry of Electronics and Information Technology (MeitY) empanelled Cloud Service Provider including Data Centre (DC) and Disaster Recovery (DR) facilities OR HA.

The Cloud Service Provider should provide for hosting infrastructure for BMC applications and co-ordinate with Application SI for the necessary software components – Servers, middleware components, network connectivity, security, compliance and governance features, web console that facilitates monitoring and query history, provide granular and summarised reporting of utilization, metrics etc.

The Service Provider shall be responsible for design, configuration, installation, migration, and setup of Cloud Infrastructure, comprising of the following, but not limited to

- Server Virtualization / Virtual Machines with OS Management and storage Management
- Cloud management portal including consumption visibility
- On demand and auto-scalable infrastructure
- Capacity Management
- Cloud Security
- Network architecture and infrastructure

3. Network Connectivity Services

The MSP should offer enterprise connectivity (Point to Point MPLS based) from on-premises network (Worli Data Centreand Municipal Head office and other offices/CSP of BMC) to the CSP and other cloud providers (if necessary) as per requirements from BMC. The citizens will avail the services and/or access the portals and other applications from the internet. To obtained maximum uptime MSP should ensure feasibility of connectivity as well as Cloud services with DC & DR or HA. MSP should quote charges for Internet bandwidth and P2P MPLS with unmetered data charges as mentioned in the commercial proposal.

The CSP / MSP should identify clear security objectives, limit external access, define service perimeters for sensitive data, manage traffic with firewall rules and use additional tools to help secure and protect BMC applications.

The MSP should share the design of the subnets with BMC DIT and application vendor teams. There should be judicious decisions while choosing public subnets, private subnets, and sizing for each.

- Public Subnets: used for components with an internet-facing presence.
- Private Subnets: used for components that should not have direct internet access.
- Subnet Sizing: Carefully consider the size of the subnets based on the expected number of users, the type of workloads, and the resources required.
- Route Tables:Create and associate unique route tables and security lists specific to each subnet.
- VM level firewalls: protect the subnets from unauthorized access and limit traffic at the VM level.
- Subnet level firewalls: Use firewalls to control inbound and outbound traffic at the subnet level.
- Monitoring and Auditing: Enable flow logs to monitor traffic passing through the subnets and help with auditing and troubleshooting.

4. Operations and Maintenance

Overall Operations and Maintenance activities including IT Helpdesk services, for proposed Cloud services as per scope of this bid document, for entire project duration. This shall include the entire solution, Cloud services, Infrastructure & networking services and other support services defined as part of the scope.

- Service-Level Agreements (SLAs): Adhere to SLAs that outline the expected levels of service. quality, including uptime, performance, and response times.
- Disaster Recovery: Clearly define the disaster recovery provisions, processes, and ability to support data preservation expectations.
- Change Management: Detailed change management documentation, regular reviews, assessments, and approvals of all necessary documentation.
- Provision for Basic Monitoring, Detailed Monitoring of Metrics, Logs etc.
- Provision for Security and Continuous Monitoring.
- Provision for Support during IT Security Audit.
- Provision for Cloud Management Portal / Self Servicing Portal.

The MSP shall maintain and manage the system (cloud solution) for the entire period of the contract and shall be fully responsible for ensuring adequate CPU processing power, memory, storage, network, internet bandwidth and monitoring of the cloud services for optimum performance of the entire cloud solution, conforming to SLAs as per the contract. During the support period, if the SERVICE PROVIDER is unable to comply with the support terms, the provider will have to a pay a penalty as specified under the SLA of this project. Post implementation support would also include support during scheduled DR drills (once every 6 months, which shall be performed by the application SI vendor of BMC), during regular operations while only replication is taking place, in disaster scenario when DR is active and operational, and during switchover and switchback.

5. Documentation and Version Control

Manage and maintain version control for all documents/ reports/ deliverables.
Documentation should be comprehensive & include:

- Product Literature
- Operating manuals
- Operator Reference manuals for each operator task
- General Specifications
- Documentation on troubleshooting

Phase-wise summary of scope of work to be delivered by the Cloud Service Provider for this project are categorized as under.

6. Pre-Implementation Scope

6.1 Inception Report

Under this phase, MSP shall do cloud and security assessment of existing infrastructure for the purpose of managed cloud hosting, DR requirement as well as Network Connectivity between BMC and Cloud DC & DR. Service Provider shall study the existing services/applications setup to be migrated, including networking, services, applications, databases, storage etc., prepare a detailed migration plan of existing production applications considered for migration to cloud. MSP will also study security requirement and prepare security baseline document in consultation with BMC and implement the same.

6.2 Project Implementation Plan

An indicative list of planning related documentation that the Service Provider should make at the onset is as follows:

- Migration Plan: Detailed migration plan with timelines, including but not limited to Network setup, Infrastructure setup, Database setup, Data migration, DR Site readiness, etc., should be shared with BMC by the Cloud Service Provider in a period of 15 working days from the date of award of work order.
- Manpower Deployment List: A list needs to be provided with resources that 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.
- Progress Monitoring Plan and Reporting Plan: Detailed Daily, Weekly, Monthly Progress Report formats along with issue escalation format approved by BMC.
- Standard Operating Procedures: Detailed procedures for operating and monitoring the Cloud site, Cloud management portal, etc.
- 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 must be via an Incident Management system.

6.3 Readiness and Risk Analysis

- Considering the criticality of the project to BMC, the Cloud Service Provider should study and submit a report of challenges envisaged from both organizational readiness standpoint,
- application readiness standpoint, integration standpoint (with existing infrastructure) and a risk standpoint.
- Successfully identifying and mitigating both technical and organization risks are a critical factor for setting up Cloud Services including Data Centre and Disaster Recovery site.
- Creating a comprehensive risk mitigation strategy outlining both preventative and compensatory actions will be necessary.

7. Implementation Scope

7.1 Project Implementation Plan

The provisioning of the Cloud Services should be strictly as per the guidelines of MeitY. The Cloud Service Provider should offer various types of cloud /managed hosting services such as:

- Design, configuration, installation, and setup of cloud site
- Provisioning of Virtual Machines along with capability to autoscale
- Patch management
- Backup & Restoration of the application VMs
- P2P connectivity between Cloud DC/DR sites and Worli Data Center
- MIS & Reports – Daily/Weekly/Monthly and Quarterly
- Real time monitoring dashboard for BMC
- VAPT reports once in six months
- SLA calculation at the time of invoice
- Maintenance & Support of cloud site/solution
- Provisioning of various IT infrastructure as required by BMC
- Project Planning & Management
- Change Management
- Co-ordination with Application SI for Middleware installation & support including Database
- The Cloud site should be within India must be as per parameters mentioned in the Pre-Qualification criteria.
- The service provider shall develop, prepare and provide a Cloud solution implementation plan. The Implementation plan shall have the detailed design and architecture, specification along with inspection and test plan, risk matrix and risk mitigation strategy, training material and documentation for all deliverables.
- The Cloud Service Provider shall be responsible for design and provisioning of required IT infrastructure, underlying system software and cloud services for deploying and hosting various applications of BMC including DR site. BMC DIT will share the list of applications that needs to be hosted on cloud infrastructure. The Bidder must gauge the Application workloads criticality, complexity and the network connectivity required. The solution should be capable of enabling automatic ‘scale in and scale out’, should be agnostic to underlying hardware, storage, network, and operating system and shall allow BMC to add/reduce cloud resources on demand basis.
- The Managed Service Provider shall be responsible for migrating existing workloads from the current Cloud service and also provision for new workloads which may be introduced during the term of the contract period.

- 24x7x365 managed support (including L1, L2, and L3 support), uptime commitment up to OS levels, managed & monitored backup and retention (as per period required by BMC), OS provisioning and management, dedicated security services operations, etc.
- Availability of server logs/records for audits
- Access to monitoring tools for measuring the service levels, application performance, server performance, storage performance and network performance.
- Review and suggest modification in disaster recovery plans and guidelines for BMC providing details.
- The FMS team (Facilities Management team – BMC vendor for managing on-premises) and Application System Integration (development) teams will support the Cloud Service provider during the deployment of applications at the Cloud Solution site.
- On expiration / termination of the contract, handover/migration of VMs, data in the cloud should be in control of BMC, the responsibility of the MSP would be to convert VMs, data and transfer to a common place so that the next Cloud Service Provider or BMC can port it.
- The P2P bandwidth required for BMC to use the applications from the Cloud site will be provided by the MSP and should be extendable as per requirement of BMC.

7.2 Migration

The scope of work of the MSP pertaining to migration of existing setup to the Cloud DC shall include but not limited to,

- The Cloud Service Provider shall provide infrastructure at DC and DR as per accepted timelines.
- The Managed Service Provider shall provide Project Manager / Co-coordinator for end-to-end migration phase till signoff from BMC and moving to BAU (Business as usual) phase.
- The Managed Service Provider shall provide complete migration of all VM's, Applications databases, data, file storage, content, etc. from BMC 's existing CSP to proposed CSP's Cloud DC-DR setup as required.
- The Managed Service Provider shall support 'As-Is' migration and refrain from asking for any changes on the application side. MSP should ensure that they get reasonable clarity about the migration activity during the pre-bid stage.MSP should understand the pre-requisites – technical clarity regarding virtual machines/database/licensing etc required for migration.
- The Managed Service Provider shall provide test Plans for verifying successful migration in co-ordination with the Application SI teams.
- The Managed Service Provider shall provide a detailed Risk Management Plan that will identify potential risks, set out possible mitigation approaches, and identifies specific tasks the MSP will undertake to help avoid identified risks connected with the Migration.
- The Managed Service Provider shall demonstrate complete architectural understanding of the existing applications and processes necessary for successful migration of the applications and data as well as continued operation and maintenance of the services.
- To enable easy migration to cloud, Department may consider up-gradation of OS & DB to latest version available in the market.

7.3 Configuration

- Upon deployment of virtual machines, the MSP has to assume full administrator access and is responsible for performing additional configuration, security hardening, vulnerability scanning, application installation, troubleshooting, patch/ upgrades deployment, BIOS & firmware upgrade as and when required.
- MSP shall ensure Preparation / Updating of the new and existing Standard Operating Procedure (SOP) documents on servers & applications deployment and hardening.
- MSP shall ensure patching of VMs on the next available patch management via change window.

- The MSP shall perform installation/ re-installation of the server operating systems and operating system utilities in the VMs.
- MSP shall make provision to monitor VM up/down status and resource utilization such as RAM, CPU, Disk, IOPS and network.
- MSP shall monitor availability of the servers, operating system & system software, and network.

7.4 DR Plan and Implementation

- MSP is responsible for Disaster Recovery Services so as to ensure continuity of operations in the event of failure of primary data centre and should meet the RPO and RTO requirements. The proposed DR tool / agent may be native or third party.
- The service parameters to be met by the DR system should focus on the Recovery Time Objective (RTO) and the Recovery Point Objective (RPO), which in business terms define the 'Interruption to Service' and 'Loss of Data' respectively. The RTO will be calculated from the time of “declaration of a disaster” up to the time by which all the applications are made fully operational & end users are able to access these applications & carry out the business operations.
- The Recovery Time Objective (RTO) shall be less than or equal to 120 minutes to enable business operations & The Recovery Point Objective (RPO) should be as:
  - Transactional / Critical Data 15 minutes
  - Applications and OS 60 minutes
- The Managed service Provider should offer dashboard to monitor RPO.
- The replication can be as per MeitY guidelines which includes both synchronous and asynchronous methods. Any lag in data replication should be clearly visible in dashboard and alerts of same should be sent to BMC.
- During normal operations, the Primary Cloud Data Centre will serve the requests. The Disaster Recovery Site will not be performing any work but will remain on standby. During this period, the compute environment for the application in DR shall be available on demand basis during a functional DR or while performing drills.
- In the event of a site failover or switchover, DR site will take over the active role, and all the requests will be routed through that site. Application data and application states will be replicated between data centres so that when an outage occurs, failover to the surviving data center can be accomplished within the specified RTO. This is the period during which the Compute environment for the application shall be equivalent to DC. The installed application instance and the database shall be usable, and the same SLAs as DC shall be applicable. The use of this Full Compute DR environment can be for specific periods during a year for the purposes of DC failure or DR Drills.
- In case of any disaster, if DR is used for 2 days or more then charges of VM will applicable as of DC.
- The security shall be for full infrastructure i.e. Cloud-DC and Cloud-DR
- The Cloud Service Provider shall deploy any tools required for solution after acquiring consent from BMC.
- The MSP shall conduct DR drill once in every six months of operation wherein the Primary DC has to be deactivated and complete operations shall be carried out from the DR Site for at least 2 days. In case DR used beyond 2 Days rate for VM of DC would be applicable. However, during the change from DC to DR-Cloud or vice-versa (or regular planned changes), there should not be any data loss.
- The MSP shall clearly define the procedure for announcing DR based on the proposed DR solution. The Managed Service Provider 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 DR.
- The MSP shall plan all the activities to be carried out during any Disaster and DR Drill. MSP should intimate BMC least 15 working days before carrying out any DR drill.

- RPO monitoring, Reporting and Events Analytics for the Disaster recovery solutions should be offered as part of the offering. BMC reserves the right to reject the Bid technically if reporting and monitoring component is overlooked by the bidder.
- MSP is required to size compute and related components for DR site according to proposed solution and mention the same in solution document and include in Bill of Quantity. The Managed Service Provider is required to mandatorily provide minimum RTO and RPO mentioned in relevant section. MSPmay offer better RTO and RPO and present the same in solution document.
- Training should be provided to the staff members and System Administrator on DR.
- MSP should provide the solution document of DR.
- MSP should have proper escalation procedure and emergency response in case of failure/disaster at Primary DC.
- MSP to coordinate with respective application/ product support vendor to support DR in event of disaster or for performing periodic maintenance & upgrade activities.
- MSP will have to demonstrate the DR site to run on hundred percent capacity for proving successful implementation of the DR site.
- BMC reserves the right, on its own or via a third-party auditor, to conduct overall testing at any point of time for the services delivered by the selected bidder.
- The selected bidder would be solely responsible for implementation of all tools and software at DR site. All costs including licenses/subscription/support for Software, OS, Replication Tools, etc. if any shall be borne by the selected bidder.
- Proposed solution should support Automated switchover/ failover facilities (during DC failure & DR Drills) to be provided and ensured by MSP. The switchback mechanism shall also be automated. The selected bidder shall also provide a tool/mechanism for BMC Cloud DC to trigger DR Failover/switchover.
- MSP shall provide support for the development of a detailed disaster recovery plan. This plan document will contain steps/procedures to switch over services to DR site in the event of invocation of disaster at DC site. Selected bidder shall also document steps for restoring services from DR site to DC site.
- Managed Service Provider shall develop appropriate policy, checklists in line with ISO 22301 certification for BCP.

C. Legal, Functional, Architectural, System Administration, Performance, Security, System Integration, Training & Documentation Requirements for Cloud Services

1. Legal requirements of Cloud Services

When considering cloud hosting for Information System, there are several legal requirements that should be taken into account. These requirements may vary depending on the jurisdiction and applicable laws. The Cloud Service Provider shall fulfill following common legal considerations for cloud hosting of Information System:

1.1 Data Protection and Privacy Laws:
- Compliance with data protection and privacy laws applicable in India.
- Ensuring appropriate data protection measures, such as encryption and access controls, are in place to safeguard transaction information.

1.2 Data Residency and Sovereignty:
- Understanding and complying with laws and regulations related to data residency and sovereignty, which dictate where data can be stored and processed. This is governed by guidelines by Government of India and hence Cloud Services must be availed from MEITY empaneled Cloud Service Provider (CSP).
- Assessing whether transaction data can be stored or processed outside of specific jurisdictions.

1.3 Confidentiality and non-disclosure:

- Implementing confidentiality and non-disclosure agreements with the Cloud ServiceProvider to protect transaction information and prevent unauthorized disclosure.

1.4 Service Level Agreements (SLAs):

- Negotiating and including SLAs that clearly define the responsibilities, obligations, and liabilities of both the Managed Service provider and the Cloud Service Provider.
- Ensuring that the SLAs address uptime, data availability, data backup and recovery, and disaster recovery procedures.

1.5 Contractual Agreements:

- Establishing clear contractual agreements between the Managed Service provider and the Cloud Service Provider, outlining the terms, conditions, and legal obligations of both parties.
- Including provisions for data ownership, data access, and data portability in case of termination of the hosting arrangement.

1.6 Audit and Compliance:

- Ensuring the Cloud Service Provider undergoes regular audits and certifications, such as ISO 27001, to demonstrate compliance with industry best practices and security standards.
- Maintaining records and documentation to demonstrate compliance with applicable laws and regulations.

1.7 Intellectual Property Rights:

- Ensuring that the Cloud Services provider's intellectual property rights, including software, applications, and databases, are protected and not infringed upon by the Cloud Service Provider.

1.8 Incident Response and Notification:

- Establishing incident response procedures and notification protocols in case of security breaches or data incidents.
- Complying with breach notification laws, which may require notifying affected individuals and relevant authorities within specified timeframes.

1.9 Data Ownership and Control:

- Ensuring that the BMC retains the ownership of the data and the Managed Service Provider/ Cloud Service Provider has limited rights to access or use the data, strictly for the purpose of providing the hosting services.

1.10 Data Retention and Destruction:

- Define data retention and destruction policies in compliance with applicable legal and regulatory requirements.
- Ensure the duration for which data will be retained and the procedures for secure data destruction when it is no longer needed as per the BMC policies
- Ensure that the Managed / Cloud Services provider adheres to these policies and has appropriate data disposal mechanisms in place.

It is crucial to consult with legal professionals and experts who specialize in Government service delivery and data protection laws to ensure compliance with specific legal requirements in BMC jurisdiction. Additionally, the Cloud Service Provider should be able to provide detailed information on their security measures, compliance certifications, and data protection practices.

2. Functional requirements of Cloud Services

When considering Cloud Services, there are several functional requirements that should be considered. These requirements focus on the capabilities and features needed to effectively host and manage the Cloud Services. The Cloud Service Provider shall fulfill following common functional requirements of Cloud Services:

2.1 Scalability and Elasticity:

- The Cloud Services should provide the ability to scale the Information System infrastructure up or down based on demand.
- It should support automatic resource provisioning and dynamic allocation of computing resources to accommodate varying workloads.

2.2 Reliability and Availability:

- The Cloud Services should ensure high availability and uptime for the Information System, minimizing downtime and service interruptions.
- It should have redundant infrastructure and data centers to provide failover capabilities and disaster recovery.

2.3 Data Backup and Recovery:

- The Cloud Services should offer robust data backup mechanisms to protect against data loss.
- It should provide regular and automated backups of Information System data and ensure quick and efficient data recovery in case of system failures or disasters.

2.4 Security and Compliance:

- The Cloud Services should implement strong security measures to protect sensitive transaction data and ensure compliance with relevant regulations or data privacy / protection laws applicable in India.
- It should offer features like encryption, access controls, intrusion detection, and prevention systems, and regular security audits.

2.5 Performance and Response Time:

- The Cloud Services should provide reliable and consistent performance for the Information System, with low latency and fast response times.
- It should have robust network infrastructure and optimized data transfer mechanisms to ensure efficient data access and processing.

2.6 Monitoring and Analytics:

- The Cloud Services should offer monitoring and analytics tools to track the performance and health of the Information System infrastructure.
- It should provide real-time monitoring of resource utilization, network traffic, and system metrics to identify potential issues and optimize performance.

2.7 Integration and Interoperability:

- The Cloud Services should support seamless integration with other systems and applications within the Information System ecosystem.
- It should provide APIs, protocols, or integration frameworks to facilitate data exchange and interoperability with external systems.

2.8 Management and Administration:

- The Cloud Services should offer a user-friendly management interface or control panel to administer and configure the Information System infrastructure.
- It should provide features for managing user access, permissions, and roles within the cloud environment.

2.9 Support and Customer Service:

- The Cloud Services should provide responsive and knowledgeable customer support to address any technical issues or concerns.
- It should offer 24/7 support, escalation procedures, and a dedicated support team familiar with functionality of department and Information System requirements.

These functional requirements will ensure that the Cloud Services can effectively meet the needs of hosting and managing allInformation Systems, providing a reliable, scalable, secure, and performant environment for data and applications.

Cloud Requirement Compliance Checklist*

The Cloud Service should comply with the below mandatory requirements:

1. **Cloud Workload: -**
   A. This includes provisioning and management of Cloud infrastructure, System Monitoring and Performance Management, Security and Compliance, Backup and Disaster Recovery, Patch and Update Management, Incident and Response Management, Co-ordination with third party vendors of Systems integrated with SAP systems, Reporting and Documentation. The provisioning of the Cloud Services shall be strictly as per the guidelines of MeitY on a MeitY empaneled Cloud Service Provider / Cloud Hosting Provider.
   B. MSP shall perform Migration Activity from existing CSP to new proposed CSP.
   C.MSP to provide CSP solution for Cloud Workload define at C-2.1.

2. One Time Implementation and Migration Charges :-

The term "One-Time Implementation and Migration Charges for Cloud" refers to the initial fees associated with moving an organization's data, applications, and workloads to the cloud. These charges typically cover the entire process of setting up the cloud infrastructure, configuring systems, and migrating existing data or applications from on-premises or legacy systems to the cloud environment.

Cloud Setup & Configuration: Setting up the cloud environment (e.g., AWS, Azure, Google Cloud) and configuring necessary resources such as virtual machines, storage, databases, networking, and security features.

Customizations: Tailoring the cloud environment to meet specific business requirements, including custom workflows, integrations with existing systems, or additional functionality.

Security Configurations: Setting up firewalls, access control, encryption, and other security measures.

Testing & Validation: Ensuring the cloud setup works as expected and meets performance, security, and compliance standards.

Data Migration: Moving data from on-premises or legacy systems to the cloud. This includes planning, extraction, transformation, and loading (ETL) of the data.

Application Migration: Migrating existing applications to the cloud, which may include refactoring or re-architecting applications to work in the new cloud environment.

System Integration: Integrating the migrated systems and applications with other services or data sources within the cloud environment or across different platforms.

Testing and Validation: Testing the migrated applications and data to ensure everything functions correctly in the cloud environment.

Sr. No	Category of Requirement	Minimum Requirement for Compliance
1	A. **LINUX virtual machine** (CentOS/Open Source OS latest version support included for the OS): B. **LINUX virtual machine** (RHEL latest version with Enterprise License support included for ethe OS) C. **Windows virtual machine** (Enterprise grade Latest Windows with Enterprise License support included for the OS) Memory :CPU:- 4vCPU : 8GB RAM (1:2	Must support variety of operating systems including Linux, Ubuntu, Windows Server, Red Hat Enterprise Linux, SUSE Linux Enterprise Server, CentOS/ Debian, etc. VMs should support both BYOL (Bring your own license) as well as PAYG (Pay as you go). The OS offered should come with continuous updates and upgrades for the entire contract duration. The Service Provider will be responsible for providing support for OS, all software and tools and the associated incidents. The Service Provider shall make arrangements with the respective OEMs accordingly. CSP should offer license portability for Windows and DB.

	ratio) HDDOS :- 100GB SSD D. **Linux virtual machine** Memory : CPU:- 16v CPU : 32GB RAM (1:2 ratio) HDD OS :- 100GB SSD GPU : 16GB E.**Windows virtual machine** Memory : CPU:- 16v CPU : 32GB RAM (1:2 ratio) HDD OS :- 100GB SSD GPU : 16GB F. G. **Linux virtual machine** Memory : ACPU:- 8 APU CPU : 32GB RAM HDD OS :- 250GB SSD H. **Windows virtual machine** Memory : APU:- 8 CPU : 32GB RAM HDD OS :- 250GB SSD	Virtual Machines shall support running a variety of workloads such as compute-intensive workload, memory-intensive workload, general-purpose workload, etc. Compute should be dynamically scalable up and down as per request from department as well as per setup with parameters such as CPU utilization of the machines. VMs should increase and decrease based on the demand (horizontal and vertical scaling). Provide facility to use different types of storage based on type of application. The CSP/MSP should offer tools to monitor VM up/down status and resource utilization such as RAM, CPU, Disk, IOPS and network The CSP/MSP should offer VMs with the latest generation processor offered by the processor OEM (Not earlier than 2019) Physical core to vCPU ratio should be minimum 1:2 for all VMs Provide facility to configure virtual machine of required vCPU, vRAM and vDisk. There should be a provision to increase storage. VMs should be firewall protected and support Host based Security Software.VM should have Endpoint Detection and Response (EDR)/Cloud Workload protection with anti-virus protection, anti-spyware, anti-malware, anti-ransomware, etc. Each VM should have a default persistence disk attached, OS disk should be bundled with 100 GB SSD. SSD should support up to 500 IOPS per disk. For Database Servers High IOPS SSD data disk to be proposed with 5000 IOPS and throughout of 200 Mbps per TB. Provide the capability to copy or clone virtual machines for archiving, troubleshooting, and testing. BMC retains the right to request full copies of virtual machines at any time. BMC retains ownership of all virtual machines, templates, clones, and scripts/applications created for BMC's applications. BMC retains ownership of BMC loaded software installed on virtual machines and any application or product that is deployed on the Cloud by BMC. In case of suspension of a running VM, the VM shall still be available for reactivation for a reasonable time (30 days) without having to reinstall or reconfigure the VM for BMC. In case of suspension beyond a reasonable time, all the data within it shall be immediately deleted / destroyed and certify the VM and data destruction for BMC as per stipulations and shall ensure that the data cannot be forensically recovered.
2.	Additional CPU/APU	Physical core to additional vCPU ratio should not be more than 1:1 for all VMs . Price shall be quoted for per Core.

3.	Additional Memory	The MSP shall provide additional memory to VM as requested by BMC . Price shall be quoted for per GB.
4.	Additional Block Storage to be attached to VM - SSD	The MSP/CSP shall provide SSD based disk storage capabilities on-demand, dynamically scalable. Each VM should have a default OS disk attached. OS Disk should be offered with bundled 100 GB SSD. SSD should support up to 500 IOPS per disk. For Database Servers High IOPS SSD data disk to be proposed with 5000 IOPS and 200 Mbps throughput per TB. CSP / MSP should support the needs of I/O-intensive workloads, particularly database workloads that are sensitive to storage performance and consistency in random access I/O throughput.
5.	File Share Storage (EFS/NAS) - between multiple virtual machines	Provide facility to configure virtual machine of required vDisk. There should be a provision to increase storage in multiples of GB.
6.	Backup Agent	The agent/service should be compatible with all OS and configuration of VM's.
7.	Backup Storage	The CSP shall configure, schedule, monitor and manage backup solution/service covering but not limited to daily, weekly, monthly, quarterly and annual backup functions (full and incremental) for data and software maintained on the VMs, disks, block storage etc. MSP should have option to restore VM using an image-based mechanism for faster commissioning of VMs. BMC should be able to recover individual files, complete folders, entire drive or complete system to source machine or any other machine available in network and facility should be available on demand 365*24*7. The service provider must ensure integrity of the data returned during a restore by verifying the block data read with a check sum of the data. MSP shall perform restoration testing quarterly with the permission of BMC The backup service must provide compressed data backup and support at least 256-bit encryption for data in transit and data at rest. Backups should be stored in such a way that disaster at either DC or DR or both should not result in loss of backups. It should be possible to restore the data from multiple storage locations independently. Provider should be able to manage multiple versions / revisions of backups.
8.	Internet Link (500Mbps)	500 mbps unshared (1:1), The delivery should be through a public IP address The MSP shall provide access of Public network/Internet to Cloud workload as per

		requirements of BMC..
9	Data Replication (Cloud DC-Cloud DR, or HA)	CSP / MSP shall have the capability to provide adequate bandwidth between Primary Data Centre and Disaster Recovery Centre or HA for data replication between VMs .
10	**SD-WAN (ISP 1)** And **SD-WAN (ISP 2)**	1.The connectivity provided by the bidder has to be MPLS/SDWAN solution on dedicated ports with 1:1leased lines committed information rate with end point. 2.All the POPs from where the SD-WAN bandwidth is provided to BMC should have redundancy at Link level and at equipment level, power, backhaul connectivity etc. 3.MSP shall provide SD-WAN connectivity as and when required by BMC for different CSP. 4.Minimum Bandwidth SDWAN(ISP 1): - Worli Data Center: - 500Mbps (1:1 ratio) CSP: - 500Mbps (1:1 ratio) 5. Minimum Bandwidth SD-WAN (ISP 2): - Worli Data Center: - 150 Mbps (1:1 ratio) CSP: - 150Mbps (1:1 ratio) The SD-WAN solution is currently implemented at 252 locations, with an additional 120 locations for the Disaster Management Department, all connected via Ninjanet SD-WAN. The following key locations require SD-WAN compliance and seamless integration with the existing Ninjanet infrastructure: Worli Data Center – ISP1 / ISP2 CSP (Cloud Service Provider) – ISP1 / ISP2 All new and existing locations must comply with the Ninjanet SD-WAN framework and support the following technical specifications: **TechnicalRequirements**: **RoutingandNetworkIntegration**: * Must support Dynamic Routing Protocols – BGP and OSPF. * Seamless integration with Ninjanet Orchestration for centralized policy and network management. **PerformanceandReliability**: **DynamicPathSelection**: * The SD-WAN solution must continuously monitor multiple network links. * Intelligent traffic routing based on real-time link performance for optimized connectivity. **AggregatedSpeedSupport**: * Must support aggregated bandwidth up to 10Gbps for high-speed connectivity.

		SecurityandCompliance: Integrated security features, including: * Encryption for secure data transmission. * Network Segmentation for isolation of critical traffic. * Cloud Security Services to safeguard data across hybrid environments. **CloudandVirtualizationSupport**: **CloudIntegration**: Seamless connectivity to major cloud platforms such as AWS, Azure, and GCP. **Overlays**: Must support multi-tenant segmentation and network virtualization for enhanced flexibility. All participating vendors must ensure their SD-WAN solution fully complies with the above-listed requirements to qualify. The proposed solution should be highly secure, scalable, and capable of seamless integration with the existing Ninjanet SD-WAN infrastructure.
11	Load Balancer as a service (5 rules)	1. MSP shall provide hardware or software based load balancer Services through a secure, hardened, redundant CSP Managed Virtual Load Balancer platform that should support up to 10 rules. 2. Load balancer shall support HTTP/HTTPS traffic and Layer 7 routing based on content (URL, headers).
12	Public IP Address	1. MSP shall provide public IP with NAT facility for cloud workload whenever asked by BMC. 2. MSP shall be responsible for providing secured exposure of internal network resources, such as servers or applications, to the internet while maintaining the privacy of internal IP addresses. The service dynamically maps private IP addresses to a public IP address, enabling secure communication between internal systems and external users or services. This solution will optimize the use of limited public IP addresses while enhancing security by keeping internal network architecture hidden from direct exposure.
13	Firewall as a Service (UTM/IPS/IDS) (assume quantity = 1 for DC and 1 for DR)	The MSP should provide security firewall with built-in high availability. It should support threat intelligence, DNS proxy, custom DNS, and web categories, IPS/IDS, Application-level filtering for https/SQL. Firewall must be able to provide intrusion prevention support along with capability to provide protection from malicious domain, domain hosting malware, domains which looks legitimate but are compromised and may host botnets etc.

14	Web Application Firewall (vWAF/cWAF) with 10 rules	1. The solution should provide protection against known vulnerabilities like OWASP Top 10 vulnerabilities, SANS Top 25 Vulnerabilities and WASC Web Security Attack classification. o It should be able to prevent all application security threats including Cross Site Scripting (XSS), SQL injection, remote file inclusion, Brute Force Attack, Buffer overflow, Cookie poisoning & Cookie Protection and Parameter tampering. 2. The WAF should allow for exception handling like Whitelisting and Blacklisting of IPs and allow blocking of IPs based on geographic location. WAF should support different policies for different web applications and allow modification of these policies upon request. 3. On request integration of new applications, increase in data transfer and throughput should be provided at quoted rates. WAF should be able to handle throughput of handling clean https traffic of up to 50 Mbps with scalability up to 1 Gbps.
15	DDOS Protection	• The service provider would offer DDOS Protection to protect the cloud infrastructure. Security solution shall protect against DDoS attack and provide mitigation. • The DDoS solution should provide protection against Layer 3, 4 volumetric attacks and Layer 7 DDoS attacks The DDoS solution should protect against emergent DDoS attack vectors such as Dynamic IP, Pulse, Burst DDoS attacks and other zero-day attack methods. • The solutions provided should have SIEM integration capability with major SIEM tools like IBM QRadar etc.
16	Wild card SSL Certificate (support unlimited sub- domains)	**MSP shall provide SSL with validity of 36 months.** **Issuer**: The entity that issued the certificate, typically a Certificate Authority (CA) like Let's Encrypt, DigiCert, or GlobalSign. **Wild card SSL Certificates**: • Secures a domain and all its subdomains. • Provide unlimited subdomain.
17	Advance Threat Protection	MSP shall provide Threat Intelligence (SaaS) typically involving real-time data, analytics, and insights about security threats, vulnerabilities, and potential attacks. These services help organizations proactively detect, analyze, and respond to emerging threats, leveraging the scalability, flexibility, and security capabilities of cloud workload.
18	P2P Cross Connect /Termination Charges	The MSP shall provide cross connect connectivity from CSP to Cloud workload ensuring network throughput as per MPLS links and inter server communications.

19	Micro segmentation	The MSP shall provide following future: Granular **Access Control**: • Micro segmentation allows for precise control over which devices or users can communicate with each other. Each workload, application, or user is isolated into its own segment with specific access controls based on identity, role, or other contextual factors. • By applying **zero-trust principles**, where no device or user is trusted by default, micro segmentation ensures that even internal network traffic is restricted unless explicitly allowed. Security **at the Workload Level**: • Traditional security models often focus on securing network boundaries, but micro segmentation shifts the focus to securing individual workloads (e.g., virtual machines, containers, or servers). This means securing each endpoint or workload independently. • Micro segmentation can be applied in both **on-premises** environments and **cloud infrastructures** (like **AWS**, **Azure**, or **Google Cloud**). Network **Traffic Control**: • Microsegmentation involves controlling and monitoring network traffic at the **east-west** layer (i.e., traffic between servers or workloads within the data center or cloud), not just at the **north-south** layer (traffic entering and exiting the data center or cloud). • It creates policies to segment traffic and restrict communication between workloads that do not need to communicate, thus reducing the risk of threats spreading across the network.
20	VMDR (Vulnerability Management, Detection, and Response)	Discovery and classification of all IT assets across cloud, on-premises, and hybrid environments. Deployment of Cloud Agents and scanner appliances where required. Configuration of scanning profiles and schedules. Integration with patch management tools for automated remediation Signatures database must be self updating. Signatures database must be searchable based on vulnerability attributes like CVE, vendor etc. Signatures must allow user updation like severity modification, adding more intelligence or even disabling a signature. It should allow to reset to system defaults if changes not needed. Signatures must be mapped to CVE ID, CVSS v2 and v3 scores, Vendor reference if any

		Signatures must have info about public exploit availability, Patch availability etc Signature database must allow to be downloaded to CSV etc Signatures must provide Real time threat information like easily exploitable, public exploit available, DoS, High lateral movement, High Data Loss etc Signatures must provide evidence of the vulnerability upon scan Must allow creation of custom signatures using OVAL etc Threat intelligence must be sourced from at least 20+ threat and exploit intelligence sources to help identify organization's unique risks and prevent attacks
21	WAS (Web Application Scanning)	Identification and onboarding of in-scope web applications. Configuration of authentication mechanisms for authenticated scanning. Setting up automated scan schedules with proper exclusions. Validation of scanning results and remediation workflows Scans should identify data disclosure vulnerabilities, such as leakage of personally identifiable information (PII). Scans should identify Flow control vulnerabilities, such as forceful browsing and cross-site request forgery (CSRF). Scans should identify Data injection and manipulation, such as SQL injection, buffer overflow, cross-site scripting (XSS) or command injection. Solution must also assist in detecting malware that might have been embedded in the website preventing customers from exposing malware infections to their customer to ensure brand reputation. Ability to customise reports for different criteria for example: 1) Web Application Report to show security status of web application combined into one report for trending details. 2) Scan Report to show results of a particular web application based on a single scan. 3) ScoreCard report to show detected vulnerabilities, sensitive contents sorted by group and rank. Ability to customize report to show vulnerabilities that are NEW,ACTIVE,Re-opened, Fixed. Ability to allow filtering to show only vulnerabilities on specific URLs in the report to focus on vulnerability remediation
22	Threat Vision	An intelligent threat detection and monitoring system that provides real time visibility, anomaly detection and pro-active threat mitigation. Provide APIs and integrations for SIEM, SOAR,

		DevSecOps pipelines, cloud security platforms, and enterprise risk management tools to enhance automated security workflows Proactive Risk Mitigation: Organizations will be able to predict, prioritize, and mitigate risks before they are exploited. Improved Security Operations Efficiency: Security teams can reduce alert fatigue by focusing only on high-risk vulnerabilities with real-world exploitability potential. Faster Response to Emerging Threats: Automated threat correlation and real-time updates ensure that organizations stay ahead of evolving threats. Enhanced Compliance & Reporting: Organizations will have better tools to track and document security posture improvements for audits and regulatory reporting. Optimized Security Investments: AI-driven insights will help security teams allocate resources effectively by addressing the most critical risks first.
23	CSPM (Cloud Security Posture Management)	Fully functional SaaS-based CSPM solution. Documentation on security policies, compliance reports, and user training. API access for third-party integrations. Ongoing technical support and training sessions Solution must be a Cloud-based SaaS platform that can be deployed globally or regionally with data residency options to meet compliance requirements. Management of the solution must be delivered over a secure platform that ensures end-to-end encryption with AES-256 for data at rest and TLS 1.3 for data in transit. The tool's architecture must incorporate an agent-less approach to reduce overhead, with processing occurring outside the customer's network to minimize resource consumption. The solution must provide a unified platform integrating CSPM, CWPP (Cloud Workload Protection Platform), CIEM (Cloud Infrastructure Entitlement Management), and DevSecOps capabilities to reduce total cost of ownership. The vendor must offer comprehensive training programs, including on-site training twice a year and unlimited access to self-paced online courses at no additional cost.
22.	MIS Reports, Helpdesk and Change Management	Service Provider should provision daily, weekly, monthly, quarterly and on-demand reports for all items described in the scope of work and line items mentioned in Bill of material including Firewall services reports such as IDS,IPS,DDOS attacks,Network bandwidth uptime, utilization,packet loss etc.Server uptime, utilization CPU memory , disk, disk performance reports etc. This also applies for 24*7*365 Helpdesk and Change Management

3. Architectural requirements of Cloud Services

When considering the architectural requirements of Cloud Services for an Information Systemproject, several factors should be taken into account. The Managed/Cloud Service Provider shall fulfill following key architectural requirements:

3.1 Scalability: The cloud hosting architecture should support scalability to accommodate the growing needs of the Information System project. It should allow for easy scaling up or down of resources based on demand to ensure optimal performance and cost-efficiency.

3.2 High Availability: The cloud hosting architecture should provide high availability to ensure uninterrupted access to the Information System system. It should include redundancy and failover mechanisms to minimize downtime and maintain system availability in the event of hardware or software failures.

3.3 Fault Tolerance: The architecture should be designed to be fault-tolerant, meaning that it can continue to function properly even if certain components or services fail. This may involve implementing redundant systems, load balancing, and automated failover mechanisms.

3.4 Security: Security is of utmost importance in an Information System project. The cloud hosting architecture should incorporate robust security measures to protect sensitive transaction data and ensure compliance with relevant regulations. This may include encryption, access controls, intrusion detection and prevention systems, and regular security audits.

3.5 Data Backup and Disaster Recovery: The architecture should include provisions for regular data backups and disaster recovery. This involves storing data in multiple geographically dispersed locations and implementing backup and recovery mechanisms to minimize data loss and facilitate quick system restoration in the event of a disaster.

3.6 Network Connectivity: The architecture should provide reliable and high-speed network connectivity to ensure efficient communication between the Information System system components and end-users. This may involve selecting appropriate network providers and implementing robust networking infrastructure.

3.7 Integration Capabilities: The cloud hosting architecture should support seamless integration with other systems and services. This allows for data exchange and interoperability between different components of the Information System ecosystem.

3.8 Monitoring and Performance Management: The architecture should include monitoring and performance management capabilities to track system performance, identify bottlenecks, and ensure optimal resource utilization. This may involve implementing monitoring tools, performance analytics, and automated alerts for proactive issue resolution.

3.9 Compliance and Regulatory Requirements: The architecture should facilitate compliance with relevant regulatory requirements, such as data privacy and security regulations. It should support features like data encryption, audit trails, and access controls to meet the specific compliance needs of the Information System project.

3.10 Cost Optimization: The architecture should consider cost optimization strategies to ensure efficient resource utilization and minimize operational costs. This may involve using cost-effective cloud service models, such as on-demand pricing, reserved instances, or spot instances.

4. System administration and management function requirements for Cloud Services

When utilizing Cloud Services, there are several system administration and management function requirements to consider. These requirements focus on the tasks and responsibilities necessary to effectively administer and manage the Information System in a cloud environment. The Managed Service Provider shall fulfill following common system administration and management function requirements for Cloud Services:

4.1 System Monitoring and Performance Management:

- Continuous monitoring of the cloud infrastructure to ensure optimal performance and resource utilization.
- Tracking and analyzing system metrics, such as CPU usage, memory usage, network latency, and disk space, to identify performance bottlenecks and optimize system performance.
- Setting up alerts and notifications for critical system metrics to proactively address any issues.

4.2 Provisioning and Configuration Management:

- Efficient provisioning of virtual machines, storage resources, and other necessary infrastructure components for the Information System.
- Managing the configuration of the cloud environment, including network settings, security groups, and access controls.
- Automating the provisioning and configuration processes to ensure consistency and reduce manual effort.

4.3 Security and Compliance Management:

- Implementing and managing robust security measures, such as access controls, firewalls, intrusion detection systems, and encryption mechanisms, to protect the Information System data and infrastructure.
- Regularly updating and patching the system with the latest security patches and software updates.
- Conducting vulnerability assessments and penetration testing to identify and address security vulnerabilities.
- Ensuring compliance with relevant regulatory requirements, such as Digital Personal Data Protection (DPDP) Act 2023 and maintaining appropriate documentation.

4.4 Backup and Disaster Recovery Management:

- Developing and implementing backup and disaster recovery strategies for the Information System data and infrastructure.
- Configuring and scheduling regular backups of critical data, applications, and configurations.
- Testing and validating the backup and restore processes to ensure data integrity and availability in the event of a disaster or system failure.
- Maintaining off-site backups and implementing replication or mirroring mechanisms for data redundancy.

4.5 Incident and Problem Management:

- Establishing processes for handling and resolving incidents and problems related to the Information System and the cloud hosting environment.
- Logging and tracking incidents and problems, prioritizing them based on severity and impact, and ensuring timely resolution.
- Conducting root cause analysis for major incidents and implementing preventive measures to minimize their recurrence.

4.6 Change and Release Management:

- Planning and managing changes to the Information System and the cloud environment in a controlled manner.
- Performing impact assessments for proposed changes and coordinating with relevant stakeholders for approvals and scheduling.
- Implementing version control and change tracking mechanisms to ensure proper documentation and accountability for system changes.

4.7 User Access and Identity Management:

- Managing user access and authentication mechanisms for the Information System and the cloud environment.
- Configuring user roles, permissions, and access controls to enforce proper data security and privacy.
- Implementing strong authentication mechanisms, such as multi-factor authentication, to protect user accounts.

4.8 Reporting and Documentation:

- Generating regular reports and documentation related to system administration and management activities, such as system performance reports, incident reports, and compliance documentation.
- Maintaining up-to-date documentation of the cloud environment, including configurations, network diagrams, and system procedures.

These system administration and management function requirements ensure that the Cloud Services are effectively managed and maintained, providing a secure, stable, and well-performing environment for data and applications.

5. Performance requirements of Cloud Services

When considering performance requirements for Cloud Services, it is important to ensure that the cloud infrastructure can deliver the necessary performance to support the system's needs. The Managed Service Provider shall fulfill following key performance requirements:

5.1 Response Time: The Cloud Services should provide low response times to ensure a smooth user experience. The Cloud Services should be responsive and provide quick access to data and functionalities.

5.2 Scalability: The cloud infrastructure should be capable of scaling resources to accommodate varying workloads. This allows the Information System to handle increased user traffic or data processing requirements without significant performance degradation.

5.3 Availability: The Cloud Services should guarantee a high level of availability, minimizing downtime and ensuring the Information System is accessible to users whenever needed. This can be achieved through redundancy, fault-tolerant architectures, and effective disaster recovery mechanisms.

5.4 Network Performance: The Cloud Services should provide robust network connectivity with high bandwidth and low latency. This ensures efficient data transfer between the Information System and its users or external systems.

5.5 Data Transfer Speed: The cloud infrastructure should support fast data transfer speeds, particularly when exchanging large volumes of data. This is essential for activities such as uploading and downloading transaction records, images, or other data.

5.6 Database Performance: If the Information System relies on a database system, the Cloud Services should ensure optimal database performance. This includes efficient query execution, indexing strategies, and appropriate database configuration to handle concurrent access and large data volumes.

5.7 Load Balancing: The cloud infrastructure should have load balancing mechanisms to distribute the workload evenly across multiple servers or instances. This helps prevent resource bottlenecks and ensures optimal performance even during peak usage periods.

5.8 Monitoring and Performance Optimization: The Cloud Services should provide monitoring tools and analytics to track system performance. This allows administrators to identify and address performance bottlenecks, optimize resource utilization, and fine-tune the Information System for optimal performance.

5.9 Storage Performance: If the Information System relies on cloud storage services, the performance of data storage and retrieval should meet the system's requirements. This includes fast access to transaction records, images, or other stored data.

5.10 Integration Performance: If the Information System integrates with external systems or APIs, the Cloud Services should ensure efficient integration and data exchange. This includes reliable and fast communication with external systems to minimize delays and support real-time data synchronization.

It is important to that the Cloud Service Provider collaborates closely with the stakeholders to understand their performance capabilities and discuss specific performance requirements for the Information System. Regular performance testing and monitoring can help identify any performance issues and allow for proactive optimization and fine-tuning of the system.

6. Security requirements of Cloud Services

When considering the security requirements of Cloud Services, it is crucial to prioritize the protection of sensitive data and ensure compliance with relevant regulations. The Managed Service Provider shall fulfill following key security requirements:

6.1 Data Encryption: The Cloud Services should provide robust encryption mechanisms to protect data at rest and in transit. This includes encryption of data stored in databases or cloud storage, as well as encryption of data transmitted over networks.

6.2 Access Control: The Cloud Services should offer strong access control mechanisms to ensure that only authorized individuals can access the Information System and its data. This includes user authentication, role-based access control (RBAC), and fine-grained permissions management.

6.3 Network Security: The cloud infrastructure should have secure network configurations, including firewalls, intrusion detection and prevention systems (IDS/IPS), and virtual private networks (VPNs). These measures help protect the Information System from unauthorized network access and mitigate the risk of network-based attacks.

6.4 Threat Detection and Prevention: The Cloud Services should have robust security monitoring systems in place to detect and respond to security threats promptly. This includes real-time monitoring of system logs, network traffic analysis, and the use of security information and event management (SIEM) tools.

6.5 Vulnerability Management: The Cloud Services should regularly assess the system for vulnerabilities and apply necessary security patches and updates. This includes conducting vulnerability scans, penetration testing, and implementing a formal patch management process.

6.6 Data Backup and Disaster Recovery: The Cloud Services should offer reliable data backup and disaster recovery mechanisms to ensure data integrity and availability in the event of system failures or disasters. This includes regular backups, off-site storage, and well-defined recovery procedures.

6.7 Recovery Point Objective (RPO) and Recovery Time Objective (RTO)

- Recovery Point Objective (RPO): RPO refers to the maximum amount of data loss that is deemed acceptable during the recovery process. It defines the point in time to which data must be recovered in order to resume normal operations. For an Information System, the RPO determines how frequently data backups or replication should be performed. A smaller RPO indicates a lower tolerance for data loss, meaning that more frequent backups or real-time replication may be required to minimize data loss in case of a failure. For this Cloud Services project the RPO required to be maintained is 15minutes.
- Recovery Time Objective (RTO): RTO is the maximum tolerable duration of time within which the Information System must be recovered and made operational after a system failure or disaster. It represents the target time for system recovery and resumption of normal operations. The RTO includes the time required for system diagnosis, data restoration, system repair, and any necessary testing or validation. Achieving a shorter RTO typically involves implementing robust backup and recovery processes, efficient system monitoring, and automated failover mechanisms. For this Cloud Services project the RTO required to be maintained is 2 hours.

6.8 Regulatory Compliance: The Cloud Services should comply with relevant regulatory requirements, such as local data protection laws. It should provide necessary safeguards and controls to protect user's privacy and ensure compliance with data protection regulations.

6.9 Security Incident Response: The Cloud Services should have a well-defined incident response plan and procedures to handle security incidents effectively. This includes prompt incident detection, containment, investigation, and communication of security breaches or incidents to relevant stakeholders.

6.10 Physical Security: The Cloud Services should have physical security measures in place to protect the data centers where the Information System is hosted. This includes access controls, video surveillance, environmental controls, and disaster-resistant infrastructure.

6.11 Security Auditing and Compliance Reporting: The Cloud Services should provide regular security audits and compliance reporting to demonstrate adherence to security standards and regulations. This includes providing audit logs, security assessment reports, and other documentation as required.

6.12 The Managed Service Provider should ensure complete security requirements for the Cloud hosting of BMC with suitable security arrangements as per MeitY guidelines. An IT security policy, framework, and operational guidelines as per ISO 27001, 27017, 27018 & PCI-DSS be maintained & implemented by Cloud service provider (CSP).

6.13 Security Policies and Standards:

6.13.1 All the security management processes, tools, and usage shall be well documented in security policy and the security best practices to be followed to maintain IT security.

6.13.2 The Managed/Cloud Service Provider shall be contractually subject to all GoI IT Security standards, policies, and reporting requirements. CSP/MSP shall meet and comply with all GoI IT Security Policies and all applicable GoI standards and guidelines, other Government-wide laws, and regulations for protection and security of Information Technology.

6.13.3 The Cloud Service Provider should meet the ever-evolving security requirements as specified by CERT-In (https://www.cert-in.org.in/).

6.13.4 The Cloud Service Provider should meet any security requirements published (or to be published) by MeitY or any standards body set up/recognized by the Government of India from time to time and notified to the Cloud Service Provider by MeitY as a mandatory standard.

6.13.5 The MSP should follow MeitY guidelines for Cloud Security Best practices and make all efforts to be in line with the latest guidelines as released from time to time.

6.14 Data Security:

6.14.1 Data shall not leave the Indian boundaries and data residing within Cloud shall not be accessed by any entity outside the control of BMC. Also, CSP/MSP should make all efforts to comply with data security acts such as DPDPA (Digital Personal Data Protection Act).

6.15 Monitoring and Access:

6.15.1 CSP/MSP should provide read-only access for monitoring of all security tools proposed and implemented for BMC including but not limited to Firewall, WAF, DDOS.

6.15.2 BMC may implement or extend any existing security solutions which are used in the current environment.

6.16 Audit and Compliance:

6.16.1 MSP shall support audit features such as what request was made, possibly the source IP address from which the request was made, who made the request, when it was made, and so on.

6.16.2 The MSP shall conduct a vulnerability and penetration test on the proposed Cloud solution every 6 months, and reports should be submitted to BMC. Corrective action should be taken by the Managed Service Provider within 3 months from the date of submission of the report. Compliance review should be done within 4 months from the date of submission of the report. Any non-compliance in the reports may lead to penalty clauses. The MSP needs to update the system in response to any adverse findings in the report, without any additional cost to BMC. BMC may also depute auditors to conduct a security check/vulnerability test/penetration test.

6.16.3 Security Audit will be performed by BMC or BMC nominated agencies as per the requirement. MSP shall provide the necessary support for the audit activity and adhere to the points highlighted by the nominated agency/BMC.

6.17 Security Controls: The Cloud Service Provider shall provide adequate security controls not limited to the measures as described below:

6.17.1 Secure Access Controls

The system shall include mechanisms for defining and controlling user access to the operating system environment and applications. Best practices from enterprise security including password strength, password aging, password history, reuse prevention etc. must be followed for access control.

6.17.2 Network Security

The Cloud Service Provider shall provide network connectivity between the server and storage with minimum permissible latency.

6.17.3 Hardening

All unnecessary packages must be removed and/or disabled from the system. Additionally, all unused operating system services and unused networking ports must be disabled or blocked. Only secure maintenance access shall be permitted, and all known insecure protocols shall be disabled.

6.17.4 Malicious Software Prevention

Implementation of EDR with anti-virus software and other malicious software prevention tools shall be supported for all applications, servers, data bases etc.

6.17.5 Logging

Logs must be maintained for all attempts to log on (both successful and unsuccessful), any privilege change requests (both successful and unsuccessful), user actions affecting security (such as password changes), attempts to perform actions not authorized by the authorization controls, all configuration changes etc.
Additionally, the access to such logs must be controlled in accordance to the least privilege concept, so that entries may not be deleted, accidentally or maliciously.
All logs should be aggregated into a central server and should be synchronized into a central Syslog server at BMC Worli data Center on a near real time basis.

6.17.6 Information Security: Log Monitoring and Correlation

All Servers / sub systems / network devices / appliances as proposed shall have capability and throw logs to the log server. The Logs and events generated by VMs, applications, DB, network, security component / devices of the system shall be monitored and may need to be integrated with the SysLog server at BMC Worli Data Center.

Regular security assessments and audits can help validate the security posture of the Cloud Services and ensure ongoing compliance with security requirements.

7. System Integration (to other existing systems)

Cloud service provider (CSP) / Managed Service Provider (MSP) shall facilitate integration of various applications deployed on Cloud by allowing access between various applications some of which may be on other Cloud Service.

8. Training and Training Materials

Training is a critical component in the successful implementation and adoption of Cloud Services. It ensures that users are equipped with the necessary knowledge and skills to effectively use the Cloud Services. The Cloud Service Provider shall provide following key training and training materials for the Cloud Services:

8.1 Training on Performance Monitoring, Reporting:
Train administrators on monitoring system performance, generating reports, and troubleshooting common issues.

8.2 Documentation and Knowledge Base: Maintain a comprehensive documentation repository and knowledge base that includes training materials, FAQs, troubleshooting guides, and best practices. This serves as a reference for users to reinforce their learning and find answers to common questions.

8.3 User Support Channels: Establish user support channels, such as a helpdesk, online ticketing system, or dedicated support team, to address user queries, issues, and requests for assistance. Prompt and efficient support is crucial in ensuring user confidence and satisfaction with the Cloud Services.

9. Documentation requirements of Cloud Services

When it comes to documentation requirements for Cloud Services, it is important to have comprehensive documentation to ensure effective system management, security, and compliance. The Managed Service Provider shall fulfill following key documentation requirements:

9.1 System Architecture and Configuration: Document the overall system architecture of the cloud hosting environment, including details of servers, networking components, storage systems, and virtualization technologies. Capture the configuration settings and parameters that are specific to the Information System deployment, such as virtual machine configurations, load balancing settings, and network configurations.

9.2 Security Documentation: Document the security measures implemented within the cloud hosting environment, including access control mechanisms, encryption methods, and network security configurations. This should include details on user access policies, authentication mechanisms, firewall rules, intrusion detection systems, and any other security features or controls in place.

9.3 Data Management and Backup: Document the data management practices, including data backup and restoration procedures within the cloud hosting environment. This should cover details such as backup schedules, retention periods, backup storage locations, and procedures for data recovery in case of a disaster or data loss.

9.4 Disaster Recovery Plan: Document the disaster recovery plan for the Information System, outlining the steps and procedures to be followed in the event of a system failure or major disruption. This should include details on data replication, failover mechanisms, recovery time objectives (RTOs), and recovery point objectives (RPOs).

9.5 Compliance Documentation: Document the compliance measures and certifications relevant to the Cloud Services. This may include documentation related to regulatory compliance standards such as local data protection laws. Maintain copies of compliance certificates, audit reports, and any other relevant documentation.

9.6 Incident Response and Handling: Document the incident response plan for the Cloud Services, outlining the steps to be followed in the event of a security breach or incident. This should cover incident detection, response, containment, investigation, and reporting procedures. Include contact details of relevant stakeholders and incident response team members.

9.7 Change Management: Document the change management processes and procedures related to the cloud hosting environment and the Cloud Services. This should cover details on how changes to the system are requested, reviewed, approved, implemented, and tested. Include change request forms, change approval records, and change implementation plans.

9.8 User Manuals and Guides: Develop user manuals and guides specifically tailored to the Information System deployment in the cloud hosting environment. These should provide detailed instructions on how to access and use the system, along with any specific features or functionalities available.

9.9 Monitoring and Performance Documentation: Document the monitoring and performance management practices within the cloud hosting environment. This should include details on the monitoring tools used, performance metrics tracked, and any performance optimization strategies or recommendations. The Cloud Service Provider / Managed Service Provider shall submit the reports on a regular basis in a mutually decided format. The Cloud Service Provider shall workout the formats for the MIS reports and gets these approved by BMC within a month of being awarded the contract. The following is only an indicative list of MIS reports that may be submitted to the BMC:

9.9.1 Daily reports

- Summary of issues / complaints logged at the Help Desk.
- Summary of resolved, unresolved and escalated issues / complaints.
- Log of backup and restoration undertaken.
- Backup Success & Failure reports.
- Server health check-up.
- Data replication report.
- Network health report.

9.9.2 Weekly Reports

- Summary of systems rebooted.
- Summary of issues / complaints logged with the OEMs.

Summary of changes undertaken in the Data Centre including major changes like configuration changes, patch upgrades, etc. and minor changes like log truncation, volume expansion, user creation, user password reset, etc.

- Hypervisor patch update status of all servers including the Virtual Machines running.
- Backup Success & Failure reports.
- Server health checkup.
- Network health report.
- Storage consumption report.

9.9.3 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.
- Backup Success & Failure reports.
- Intrusion attack and prevention report.
- Server health check-up.
- Network health report.
- Storage consumption report.
- Patch management report.

9.9.4 Quarterly Reports

- Consolidated component-wise availability and resource utilization.
- All relevant reports required for calculation of SLAs.
- The MIS reports shall be in-line with the SLAs and the same shall be scrutinized by BMC.
- Intrusion attack and prevention report.
- Storage consumption report.

9.9.5 On Demand Reports

- Yearly Backup Success & Failure reports.
- Intrusion attack and prevention report.
- Storage consumption report.
- DR Drills report.
- DR Recovery report.
- IP and User Logs.

The Cloud Service Provider / Managed Service Provider will also provide any other report requested by BMC or any other agency approved and authorized by BMC.

9.10 Support and Contact Information: Maintain an up-to-date list of support contacts, including the Cloud Services provider's support team and any third-party vendors or consultants involved in supporting the Cloud Services. Include contact information, escalation procedures, and response time expectations.

Regularly review and update the documentation as the Cloud Services evolves, and ensure that it remains accessible to relevant stakeholders. Effective documentation helps ensure smooth system management, troubleshooting, and compliance with applicable regulations and standards.

D. Network and Communications Requirements for Cloud Services

1. Legal requirements of networking for Cloud Services project

When implementing Cloud Services, there are several legal requirements related to networking that need to be considered to ensure compliance and protect sensitive data. The Managed Service Provider shall fulfill following key legal requirements for networking in an Cloud Services project:

1.1 Data Privacy Laws: Comply with applicable data privacy laws and regulations, such as the Digital Personal Data Protection (DPDP) Act 2023. These laws govern the collection, storage, and processing of personal health information and impose strict requirements on data protection, access controls, and data breach notification.

1.2 Network Security: Implement appropriate security measures to protect the Cloud Services network and data from unauthorized access, data breaches, or other security incidents. This includes using firewalls, intrusion detection and prevention systems, access controls, encryption, and regular security assessments.

1.3 Access Controls: Implement strong access controls to ensure that only authorized personnel have access to the Cloud Services network and data. This includes unique user accounts, strong passwords, role-based access controls, and regular user access reviews.

1.4 Network Monitoring: Implement network monitoring and logging mechanisms to detect and respond to security incidents, unauthorized access attempts, or other network anomalies. Monitoring can help identify and mitigate potential security threats and ensure compliance with legal requirements.

1.5 Data Transmission Encryption: Use encryption technologies, such as Secure Sockets Layer (SSL) or Transport Layer Security (TLS), to secure the transmission of sensitive data over the network. This helps protect data from unauthorized interception or tampering during transmission.

1.6 Network Resilience and Redundancy: Implement network redundancy and failover mechanisms to ensure the availability and resilience of the Cloud Services network. This may include redundant network connections, load balancing, backup systems, and disaster recovery plans.

1.7 Compliance with Telecommunications Laws: Comply with applicable telecommunications laws and regulations, such as those governing the use of wireless communication or telecommunication services. Ensure that any telecommunication services used in the Cloud Services project comply with relevant laws and regulations.

1.8 Intellectual Property Rights: Ensure that the networking infrastructure and technologies used in the Cloud Services project do not infringe upon any intellectual property rights of third parties. This includes using licensed software, adhering to copyright laws, and respecting intellectual property rights associated with networking technologies.

1.9 Network Documentation: Maintain proper documentation of the Cloud Services network, including network diagrams, configurations, IP address management, and inventory of network devices. This documentation is essential for compliance, troubleshooting, and network management purposes.

1.10 Contractual Agreements: Ensure that any contractual agreements with network service providers or vendors include provisions for compliance with legal requirements, data protection, security controls, confidentiality, liability, and dispute resolution.

It is important to consult with legal experts who specialize in functional services and technology laws to ensure that the networking implementation in the Cloud Services project complies with applicable legal requirements. Additionally, regularly review and update network security measures and policies to adapt to evolving threats and changes in regulations.

2. Functional requirements of networking and communication for Cloud Services project

The Managed Service Provider shall fulfill following common functional requirements:

2.1 Network Infrastructure: The Cloud Services project requires a robust and reliable network infrastructure to support seamless communication and data transfer between various components of the system. This includes the deployment of switches, routers, access points, and other networking equipment to establish a secure and high-performing network.

2.2 Network Connectivity: The Cloud Services project needs to ensure stable and high-speed connectivity uptothe BMC data centre. This includes establishing wired and wireless connections to enable communication between different departments, units, and devices within the facility.

2.3 Data Security: The network infrastructure must implement strong security measures to protect sensitive transaction information and prevent unauthorized access. This includes implementing firewalls, intrusion detection and prevention systems, virtual private networks (VPNs), and encryption mechanisms to safeguard data during transmission.

2.4 Interoperability: The networking and communication components of the Cloud Services should support interoperability standards to enable seamless integration with other systems and external entities. This facilitates the exchange of data with other service providers or systems.

2.5 Scalability: The network infrastructure should be scalable to accommodate the growing needs of the user departments. As the Cloud Services expands and more users and devices are added to the network, it should be able to handle the increased traffic and maintain optimal performance.

2.6 Quality of Service (QoS): The network should prioritize traffic based on the specific needs of the Cloud Services. Critical data, such as real-time transaction monitoring or emergency communication, may require higher bandwidth and lower latency to ensure timely and reliable delivery.

2.7 Network Monitoring and Management: The Cloud Services project should include tools and processes for monitoring and managing the network infrastructure. This enables proactive identification and resolution of network issues, performance optimization, and capacity planning.

2.8 Voice and Video Communication: The networking requirements should consider the need for voice and video communication within the department/s. This may involve implementing Voice over IP (VoIP) solutions, video conferencing capabilities, and ensuring sufficient network bandwidth to support real-time communication.

2.9 Mobile Connectivity: If the Cloud Services includes mobile devices or supports mobile applications, the network infrastructure should provide reliable and secure connectivity for these devices. This may involve implementing wireless access points, mobile device management (MDM) solutions, and ensuring seamless roaming within the facility.

2.10 Disaster Recovery and Redundancy: The networking requirements should include provisions for disaster recovery and redundancy to ensure continuous operation of the Cloud Services in case of network failures or disruptions. This may involve implementing backup network connections, redundant hardware, and failover mechanisms.

These functional requirements should be analyzed and customized based on the specific needs and constraints of BMC while implementing the Cloud Services project. It is crucial to involve network specialists and IT professionals with expertise in network systems to design and implement a robust networking and communication infrastructure that meets the functional requirements and aligns with industry best practices.

3. Architectural requirements of networking and communication for Cloud Services project

The architectural requirements of networking and communication for an Cloud Servicesproject play a crucial role in ensuring a reliable, secure, and scalable infrastructure. The Managed Service Provider shall fulfill following key architectural requirements:

3.1 Network Topology: Determine the appropriate network topology for the Cloud Services project, such as a star, ring, or mesh topology, based on the facility's size, layout, and connectivity needs. Consider factors such as scalability, ease of management, and fault tolerance when designing the network topology.

3.2 Network Segmentation: Implement network segmentation to divide the network into separate segments or VLANs (Virtual Local Area Networks) based on functional or security requirements. This helps isolate critical systems, such as transaction data storage and management, from non-sensitive areas of the network.

3.3 Redundancy and Resilience: Design the network architecture with redundancy and resilience in mind to minimize single points of failure and ensure continuous operation. Implement redundant network links, switches, and routers to provide backup paths in case of network failures.

3.4 Scalability: Consider the scalability requirements of the Cloud Services project to accommodate the growing number of users, devices, and data traffic. Plan for future expansion by incorporating scalability features such as modular network switches, adjustable bandwidth capacities, and flexible addressing schemes.

3.5 Network Security: Incorporate robust security measures into the network architecture to protect sensitive transaction data and ensure compliance with applicable regulations. Implement firewalls,

intrusion detection and prevention systems, access controls, and encryption protocols to secure the network infrastructure.

3.6 Quality of Service (QoS): Define and prioritize network traffic based on the specific requirements of the Cloud Services. Assign appropriate levels of bandwidth, latency, and packet prioritization to ensure reliable and optimal performance for critical applications such as real-time system monitoring or video conferencing.

3.7 Network Monitoring and Management: Include mechanisms for monitoring and managing the network infrastructure to ensure its health, performance, and security. Implement network monitoring tools, centralized management systems, and logging mechanisms to detect and address network issues promptly.

3.8 Integration with External Systems: Plan for the integration of the Cloud Services network with external systems. Ensure that the network architecture supports the necessary protocols, interfaces, and data exchange mechanisms required for seamless interoperability.

3.9 Wireless Network Design: If the Cloud Services project includes wireless connectivity, design and deploy a secure and reliable wireless network infrastructure. Consider factors such as coverage, capacity, and interference mitigation techniques to provide consistent and robust wireless connectivity within the department/s.

3.10 Network Documentation: Maintain comprehensive documentation of the network architecture, including network diagrams, configurations, IP addressing schemes, and connectivity details. This documentation aids in troubleshooting, future expansion, and compliance with regulatory requirements.

It is important to involve experienced network architects or consultants with expertise in network systems to design and implement the networking and communication architecture for the Cloud Services project. They can ensure that the architectural requirements are met, align with industry best practices, and adhere to relevant standards and regulations.

4. System administration and management function requirements of networking and communication for Cloud Services project

The system administration and management function requirements of networking and communication for an Cloud Services project are crucial for ensuring the smooth operation, maintenance, and optimization of the network infrastructure. The Managed Service Provider shall fulfill following key requirements in this area:

4.1 Network Monitoring: Implement network monitoring tools and systems to continuously monitor the performance, availability, and security of the network infrastructure. This includes monitoring network devices, bandwidth utilization, network traffic, and security events to identify and address potential issues proactively.

4.2 Configuration Management: Establish robust configuration management practices to effectively manage network devices, including switches, routers, firewalls, and access points. This involves maintaining an inventory of network devices, documenting configurations, and implementing standardized configuration templates to ensure consistency and ease of management.

4.3 Network Troubleshooting and Support: Develop processes and procedures for troubleshooting network issues and providing timely support to address network-related problems. This includes establishing a help desk or support team to respond to network-related incidents, diagnosing and resolving connectivity issues, and escalating complex problems to specialized network engineers if needed.

4.4 Network Performance Optimization: Regularly assess and optimize network performance to ensure optimal operation of the Cloud Services. This includes monitoring network traffic patterns, identifying and resolving performance bottlenecks, optimizing network configurations, and implementing Quality of Service (QoS) measures to prioritize critical applications and traffic.

4.5 Network Security Management: Implement comprehensive network security management practices to protect the Information System and sensitive transaction data from security threats. This involves regularly updating network security policies, monitoring for vulnerabilities and attacks, applying patches and updates to network devices, and maintaining robust access controls and authentication mechanisms.

4.6 Change Management: Establish change management processes to manage and control changes to the network infrastructure. This includes documenting and reviewing proposed changes,

assessing their impact on the network, testing changes in a controlled environment, and implementing changes in a controlled and coordinated manner to minimize disruptions and maintain system stability.

4.7 Backup and Disaster Recovery: Implement backup and disaster recovery strategies for the network infrastructure to ensure business continuity in the event of network failures or disasters. This involves regularly backing up network device configurations, maintaining off-site backups, and developing recovery procedures to restore network services quickly and efficiently.

4.8 Capacity Planning: Perform regular capacity planning exercises to anticipate future network resource requirements and ensure that the network infrastructure can handle the expected growth in users, devices, and data traffic. This includes analyzing historical usage data, forecasting future demands, and making necessary adjustments to network capacity, such as upgrading hardware or adjusting bandwidth allocations.

4.9 Vendor Management: Manage relationships with network equipment vendors, service providers, and contractors to ensure effective support, maintenance, and collaboration. This includes establishing service level agreements (SLAs), coordinating equipment repairs or replacements, and staying informed about new technologies and updates that may benefit the network infrastructure.

4.10 Documentation and Reporting: Maintain comprehensive documentation of network configurations, changes, troubleshooting procedures, and performance metrics. This documentation serves as a reference for system administrators, facilitates knowledge sharing, and supports compliance requirements and audits.

By incorporating these system administration and management function requirements into the Cloud Services project, BMC department/s can effectively manage and maintain the networking and communication infrastructure, ensuring optimal performance, security, and reliability for the Information System.

5. Performance requirements of networking and communication for Cloud Services project

The performance requirements of networking and communication for an Cloud Services project are critical to ensure efficient and reliable access to information. The Managed Service Provider shall fulfill following key performance requirements:

5.1 Bandwidth: Determine the required bandwidth capacity to support the expected data traffic within the Cloud Services. Consider factors such as the number of users, types of data being transmitted (e.g., images, audio, video), and the desired responsiveness of the system. Ensure that the network infrastructure provides sufficient bandwidth to handle peak loads and minimize latency.

5.2 Latency: Define acceptable latency levels for real-time communication and data retrieval within the Cloud Services. Minimize latency to ensure timely access to information, especially for critical applications such as telemedicine, real-time monitoring, or remote consultations. Low-latency connections are essential for delivering a seamless user experience and facilitating efficient workflows.

5.3 Reliability: The networking and communication infrastructure should provide high reliability to ensure uninterrupted access to the Cloud Services. Implement redundancy and failover mechanisms to minimize downtime and mitigate the impact of network failures. This may involve redundant network links, backup power systems, and redundant network devices to ensure continuous operation.

5.4 Scalability: Plan for the scalability requirements of the Cloud Services project to accommodate the growing number of users, devices, and data traffic. The network infrastructure should be scalable to handle increased demand without compromising performance. Consider the ability to add additional network resources, such as switches, routers, and access points, as needed to support the expanding Cloud Services environment.

5.5 Quality of Service (QoS): Define and prioritize network traffic based on the specific requirements of the Cloud Services. Allocate appropriate levels of bandwidth, latency, and packet prioritization to critical applications, such as real-time video conferencing, medical imaging, or data transfers. QoS mechanisms can ensure that high-priority traffic receives the necessary network resources and prioritization over less critical traffic.

5.6 Network Response Time: Define acceptable network response time for various Information System functions, such as retrieving transaction records, accessing test results, or generating

reports. Minimize response time to enhance user productivity and satisfaction. This requires optimizing network configurations, reducing latency, and ensuring efficient data transfer across the network.

5.7 Security Performance: Ensure that the networking and communication infrastructure can handle the required security measures without compromising performance. This includes implementing firewalls, intrusion detection and prevention systems, and encryption protocols to protect sensitive data. Performance considerations should include the overhead of security protocols and mechanisms.

5.8 Data Transfer Speed: Consider the speed of data transfers within the Information System, especially for large files such as medical images or bulk data uploads. The network infrastructure should support high-speed data transfers to enable efficient sharing and retrieval of transaction information and other relevant data.

5.9 Network Monitoring and Optimization: Implement network monitoring tools and performance optimization techniques to proactively identify and address network performance issues. Regularly monitor network traffic, analyze performance metrics, and optimize network configurations to maintain optimal performance levels.

5.10 Network Resilience: Design the networking and communication infrastructure to be resilient and capable of recovering quickly from network disruptions or failures. Implement fault-tolerant mechanisms, such as redundant links, network load balancing, and failover systems, to minimize the impact of network outages on the Information System performance.

By incorporating these performance requirements into the design and implementation of the networking and communication infrastructure, BMC department/s can ensure that the Cloud Services operate efficiently, providing fast and reliable access to information for improved service delivery.

6. Security requirements of networking and communication for Cloud Services project

The security requirements of networking and communication for an Cloud Services project are critical to safeguard sensitive transaction data and protect the integrity, confidentiality, and availability of the information. The Managed Service Provider shall fulfill following key security requirements:

6.1 Access Control: Implement strong access control measures to ensure that only authorized individuals can access the Cloud Services and related network resources. This includes user authentication mechanisms such as passwords, multi-factor authentication, and role-based access control (RBAC) to enforce appropriate access privileges based on user roles and responsibilities.

6.2 Encryption: Encrypt sensitive data transmitted over the network to protect it from unauthorized interception or disclosure. Use secure protocols, such as SSL/TLS, for encrypting data in transit. Additionally, ensure that data at rest, such as stored transaction records and backups, are also encrypted to provide an extra layer of protection.

6.3 Network Segmentation: Segment the network into secure zones or virtual LANs (VLANs) to isolate different types of traffic and restrict unauthorized access between network segments. This helps contain potential security breaches and limits lateral movement within the network.

6.4 Intrusion Detection and Prevention: Deploy intrusion detection and prevention systems (IDS/IPS) to monitor network traffic, detect and block suspicious or malicious activities. These systems can help identify and respond to potential threats, including network-based attacks, malware, and unauthorized access attempts.

6.5 Firewalls: Implement firewalls to enforce access control policies and protect the network from unauthorized access or malicious traffic. Configure firewalls to allow only necessary network traffic and block potential threats, such as unauthorized incoming connections or malicious outbound traffic.

6.6 Secure Remote Access: If remote access to the Information System is required, implement secure remote access mechanisms such as Virtual Private Network (VPN) solutions. Ensure that remote access connections are encrypted and require strong authentication to prevent unauthorized access to the Information System and the network.

6.7 Network Monitoring and Logging: Deploy network monitoring tools and establish comprehensive logging mechanisms to track network activity, identify security incidents, and facilitate forensic analysis in case of security breaches. Regularly review and analyze network logs to detect and respond to security events promptly.

6.8 Security Patch Management: Regularly apply security patches and updates to network devices, including routers, switches, firewalls, and intrusion detection/prevention systems. Keep abreast of vendor security advisories and promptly apply patches to address known vulnerabilities and protect the network infrastructure.

6.9 Security Awareness and Training: Conduct regular security awareness and training programs for all personnel accessing the Cloud Services. Educate users about security best practices, such as creating strong passwords, recognizing phishing attempts, and avoiding unauthorized disclosure of sensitive information.

6.10 Incident Response and Disaster Recovery: Develop and implement an incident response plan to effectively respond to security incidents and breaches. This includes defining roles and responsibilities, establishing communication channels, and outlining procedures for containing, investigating, and mitigating security incidents. Additionally, establish robust backup and disaster recovery mechanisms to ensure the availability and integrity of the Information System in the event of a security incident or disaster.

It is essential to work closely with cybersecurity professionals and follow industry best practices to ensure that the networking and communication infrastructure of the Cloud Services project meets the necessary security requirements. Regular security assessments, penetration testing, and ongoing security monitoring should also be conducted to identify and address any vulnerabilities or risks.

7. Documentation requirements of networking and communication for Cloud Services project

Documentation plays a crucial role in capturing the design, implementation, and management aspects of the networking and communication infrastructure for an Cloud Services project. The Managed Service Provider shall fulfill following essential documentation requirements for networking and communication:

7.1 Network Design Documentation: Document the overall network design, including network topology, hardware components, and network addressing schemes. This documentation should provide a clear understanding of how the network is structured and interconnected.

7.2 Network Diagrams: Create network diagrams that visually represent the network infrastructure, including routers, switches, firewalls, access points, and their interconnections. These diagrams help in understanding the network layout, identifying potential bottlenecks, and troubleshooting network issues.

7.3 Network Configuration Documentation: Document the configuration details of network devices, including routers, switches, firewalls, and wireless access points. This includes information such as IP addresses, VLAN configurations, routing protocols, access control lists (ACLs), and security settings. This documentation helps in managing and maintaining network devices and ensures consistency across the network.

7.4 Network Security Policies and Procedures: Document the security policies and procedures related to networking and communication. This includes information on access control mechanisms, firewall rules, encryption protocols, remote access policies, and incident response procedures. These documents serve as a reference for implementing and enforcing security measures.

7.5 Network Service Level Agreements (SLAs): Document the agreed-upon service levels for network performance, availability, and response time. This includes metrics, targets, and responsibilities for monitoring and maintaining network performance. SLAs help in managing expectations and holding service providers accountable.

7.6 Network Inventory: Maintain an inventory of network equipment, including hardware models, serial numbers, firmware versions, and warranty information. This documentation helps in tracking the lifecycle of network devices, managing support and maintenance contracts, and ensuring timely updates and replacements.

7.7 Network Monitoring and Management Documentation: Document the procedures and tools used for network monitoring and management. This includes details about network monitoring systems, alerting mechanisms, log management, and performance optimization strategies. This documentation assists in troubleshooting network issues, analyzing performance trends, and maintaining network health.

7.8 Network Incident and Change Management: Document procedures and processes for handling network incidents and implementing changes to the network infrastructure. This includes incident

response plans, change control procedures, and documentation templates for recording incident details, change requests, and their outcomes. These documents promote consistency, traceability, and accountability in managing network incidents and changes.

7.9 Network Testing and Validation: Document the procedures and results of network testing and validation activities. This includes test plans, test cases, and test results for network performance, security, and scalability testing. These documents provide evidence of the network's compliance with defined requirements and standards.

7.10 Network Troubleshooting Guides: Develop troubleshooting guides or knowledge base articles that capture common network issues, their potential causes, and recommended resolution steps. These guides assist network administrators in diagnosing and resolving network problems efficiently.

It is important to maintain documentation in a central repository, ensure it is regularly updated, and make it easily accessible to relevant stakeholders. Proper documentation ensures knowledge transfer, facilitates troubleshooting and maintenance activities, and provides a valuable resource for future enhancements or upgrades to the networking and communication infrastructure of the Cloud Services project.

E. Monitoring Tool Requirements for Cloud Services

Monitoring tool requirements for the Cloud Services project should include following monitoring capabilities for Cloud Services, network and communication services and end devices:

3. Real-time Monitoring: The tool should provide real-time monitoring capabilities to track the performance and availability of critical components in the Cloud Services infrastructure.
4. Health Monitoring: The tool should be able to monitor the health of servers, databases, networking devices, and other infrastructure components, alerting administrators of any issues or anomalies.
5. Resource Utilization Monitoring: It should be able to monitor resource utilization metrics such as CPU usage, memory usage, disk space, and network bandwidth to identify potential bottlenecks or capacity issues.
6. Application Performance Monitoring: The tool should provide insights into the performance of Information System applications, including response times, transaction volumes, and resource consumption, to ensure optimal performance.
7. Alerting and Notification: The monitoring tool should have robust alerting capabilities to notify administrators and stakeholders promptly when predefined thresholds or conditions are breached. Alerts can be sent via email, SMS, or other communication channels.
8. Dashboard and Reporting: A user-friendly dashboard and reporting feature should be available to visualize key performance indicators, generate reports, and analyze historical data for capacity planning and performance optimization.
9. Event Logging and Auditing: The tool should have the ability to log events and provide an audit trail of activities for troubleshooting, compliance, and security purposes.
10. Scalability: The monitoring tool should be scalable to handle the growing needs of the Cloud Services project, accommodating an increasing number of monitored components and data points.
11. Integration Capabilities: It should be able to integrate with other systems and tools within the Cloud Services ecosystem, such as ticketing systems, log management tools, and configuration management databases, to enable seamless data exchange and correlation.
12. Security and Access Control: The monitoring tool should have robust security features, including role-based access control, authentication, and encryption, to ensure the confidentiality and integrity of monitoring data.
13. Customization and Extensibility: The tool should allow customization and extensibility to meet the specific monitoring requirements of the Cloud Services project, including the ability to create custom metrics, dashboards, and alerts.
14. Historical Data Storage: Sufficient storage capacity should be available to retain historical monitoring data for analysis, trend identification, and compliance purposes.
15. Cloud Management Portal / Self Servicing: Cloud Management Portal must have below mentioned features including but not limited to for monitoring and management.

    - Virtual Machine

- Networking
- Security Solution
- Backup Management
- DR Site (RPO, Replications, etc.)
- Storage
- Monitoring
- Load Balancer

13.1 The service provider shall provide Self Service Provisioning Portal and monitoring tool through a web browser to remotely administer their virtual instances having fine-grained role-based access controls.

13.2 It shall make the Management Reports described in this Bid accessible via online interface. These reports shall be available for the full period of the contract after being created.

13.3 The Cloud Service Provider shall provide for automatic monitoring of resource utilization and other events such as failure of service, degraded service, etc. via service dashboard or other electronic means.

13.4 The CSP / MSP shall have monitoring tools for measuring the utilization of servers, storage, and network. The tool shall be capable of providing the exact utilization of servers and shall be able to generate per day, per month and per quarter utilization reports based on which the payments will be made. The CSP / MSP should also provide access to this tool to BMC IT Dept.

13.5 Detailed user level or user group level auditing, monitoring, metering, accounting, and quota is essential for the cloud platform to be offered.

13.6 The Utilization Monitoring tools shall have minimum following features:

- Performance monitoring, thresholds, health checks and alerts.
- Historical Performance Reports.
- Capacity Utilization statistics.
- Cloud Resource Usage including increase / decrease in resources used during auto-scale.
- RPO Monitoring.
- Resource Utilization: CPU, RAM, Disk, IOPS, etc.

13.7 MSP shall provide solution to raise a trouble ticket via mail, phone and web portal.

13.8 It shall support both horizontal as well as vertical Scaling of VM's.

When selecting a monitoring tool for a Cloud Services project, it is important to consider the specific needs and requirements of the project, the complexity of the infrastructure, and the scalability and flexibility of the tool to accommodate future growth and changes.

F. TESTING AND QUALITY ASSURANCE REQUIREMENTS

3. Pre-commissioning Tests for Cloud Services

Pre-commissioning tests for Cloud Services are conducted to ensure that the system is properly installed, configured, and ready for operational use. These tests help identify any issues or discrepancies before the system goes live. The Managed Service Provider shall conduct following common pre-commissioning tests for the Cloud Services in consultation with users wherever necessary:

1.1 Test Planning and Strategy:

- Develop a comprehensive test plan that outlines the testing approach, objectives, scope, and schedule.
- Identify the test environments and resources required for testing.
- Define the test strategy, including the types of testing to be performed (e.g., functional, performance, security) and the level of automation.

1.2 Installation and Configuration Test: Managed Service Provider shall provide assistance to Information System vendor to verify that the Information Systemsare installed correctly on the designated servers. Ensure that all necessary components and modules are installed, and that the system is properly configured as per the Cloud Service Provider's guidelines. The testing includes Virtual Machine Testing, CPU and RAM Benchmarking Testing, Storage / Disk Input Output Operations Per Second (IOPS) Testing, Read/Write Latency Testing, Network Throughput and Latency Testing etc.

1.3 Performance and Load Test: Managed Service Provider shall provide assistance to Information System vendor to assess the performance of the Information System under normal and peak load conditions. Measure response times for various operations and transactions to ensure acceptable performance levels. Conduct stress testing to determine the system's stability and scalability by simulating high user loads and heavy data processing.

1.4 Security and Access Control Test: Validate the security measures implemented in the Cloud Services. Test user authentication and access control mechanisms to ensure that user permissions are properly enforced. Conduct penetration testing to identify vulnerabilities and assess the Cloud environment's resilience against security threats. Testing includes Firewall Policy and Configuration Testing.

1.5 Disaster Recovery Test: Test the Information System's disaster recovery mechanisms and backup/restore procedures. Simulate data loss or system failure scenarios to ensure that backups are available and can be successfully restored. Verify the system's ability to recover and resume normal operations in the event of a disaster. The testing includes Data Replication Testing, Data Integrity Testing, Reverse Replication Testing, Switch Over Testing etc.

The Managed Service Provider shall allocate dedicated resources, time, and expertise for testing and quality assurance activities to ensure that the Cloud Services meet the desired quality standards and user expectations. The testing process should be well-documented, and any issues or bugs should be tracked, reported, and resolved in a timely manner.

4. Operational Acceptance Tests for Cloud Services

Operational Acceptance Testing (OAT) for Cloud Services is conducted to ensure that the Information Systems are ready for operational use and meets the requirements of the BMC department/s. OAT focuses on validating the overall functionality, performance, and usability of the Information System in a production-like environment. The Managed Service Provider shall conduct the operational acceptance tests in the following key areas for theInformation System:

2.1 Test Environment:

- Set up a dedicated test environment that closely resembles the production environment where the Information System will be deployed.
- Configure hardware, software, and network components to mirror the production environment as closely as possible.

2.2 Performance and Response Time: Measure the system's performance under realistic operational conditions. Conduct tests to validate response times for common tasks and operations, such as searching for transaction records, generating reports, or processing large volumes of data. Ensure that the Information System meets performance requirements and operates within acceptable timeframes.

2.3 Security and Access Controls: Verify that the Cloud Services have appropriate security measures in place to protect transaction data and ensure authorized access. Evaluate the system's compliance with relevant data privacy and security regulations.

2.4 Error Handling and Fault Tolerance: Assess how the Cloud Services handle errors, exceptions, and system failures. Test scenarios that simulate various error conditions, such as network connectivity issues, database failures and recovers from failures without data loss or corruption.

2.5 Integration and Interoperability: Validate the interoperability of the Information System with other systems and devices within the BMC department's environment. Test the system's ability to exchange data with other relevant systems.

By conducting comprehensive Operational Acceptance Testing, the Cloud Service Providershall identify any potential issues, gaps, or areas for improvement before the system is deployed in a production environment.

G. SERVICE SPECIFICATIONS – OPERATIONS & MAINTENANCE

1. Post Deployment Support for Issue Resolution

The Managed Service Provider is responsible for resolving issues that occur during the Cloud Service contract period. Cloud Service Provider shall follow and adhere to ITIL guidelines and process for the Incident management and Problem management. The Managed Service Provider shall adopt following general steps involved in providing the required support:

1.1 Issue Identification: The BMC user identifies an issue in the Cloud Service that is covered under the contract. The issue can be reported by end-users, system administrators, or IT staff who have encountered a problem while using the Information System / Cloud Services.

1.2 Issue Reporting: The identified issue is reported to the Managed/Cloud Service Provider or their technical support team. The reporting process typically involves providing detailed information about the problem, including error messages, steps to reproduce the issue, and any other relevant information that can help the Cloud Service Provider understand and reproduce the defect.

1.3 Vendor Evaluation: The Cloud Service Provider reviews the reported issue to determine whether it falls within the scope of the support. They may ask for additional information to further investigate the problem.

1.4 Issue Resolution: Once the Cloud Service Provider confirms that the reported issue is covered under the support, they work to resolve the defect. This can involve, configuration adjustments, or hardware repairs/replacements, depending on the nature of the issue. The Cloud Service Provider may provide updates or patches to address the defect.

1.5 Testing and Verification: After the Cloud Service Provider implements the fix or resolution, they typically conduct testing to ensure that the defect has been successfully addressed and the Information System is functioning correctly. This may involve running test cases, validating the fix against the reported issue, and conducting regression testing to ensure that the resolution has not introduced new problems.

1.6 Deployment of Fix: Once the resolution is validated, the Cloud Service Provider provides instructions for applying the fix or update to the Information System environment. The BMC department or the IT staff of the Cloud Service Provider follow the provided instructions to implement the fix, ensuring that it is correctly applied to all affected components of the Information System.

1.7 Confirmation of Resolution: The BMC user verifies that the defect has been resolved by retesting the affected functionality in the Information System. They ensure that the fix has successfully resolved the issue and that the system is functioning as expected.

1.8 Documentation and Closure: The Cloud Service Provider shall maintain proper documentation of the defect, the resolution process, Root Cause Analysis (RCA)and any relevant communication related to the defect repair. Once the defect is successfully resolved, the issue is considered closed, and both parties acknowledge the completion of the warranty repair process.

1.9 Incident Management Process & Procedure

1.9.1 Monitoring Team to carry out daily Server health checkups on all the servers, storage and network devices during non-business hours of BMC. For all issues observed during server health checkup in non-business hours, the issues should

be dealt as Incident and Incident Management process and procedures should be invoked.

1.9.2 For all Incidents / Issues with Severity 'Critical and High', the Incident Management Team should be activated to provide resolution as per defined SLA's and closure of Incident. Incident Management Team will be responsible to send an Incident Report on daily basis for all such Incidents to all the stake holders including BMC designated officials.

1.9.3 For any re-occurring issue, the Problem Management Process should be initiated and problem Ticket to be created for the same. After permanent resolution of the re-occurring issue / problem, the problem ticket report shall be sent to all the stake holders.

2 Post Deployment Support for Operations

2.1 Ongoing Support and Maintenance: The Managed Service Provider shall maintain and manage the system (cloud solution) for the entire period of the contract and shall be fully responsible for ensuring adequate CPU processing power, memory, storage, network, internet bandwidth and monitoring of the cloud services for optimum performance of the entire Cloud solution conforming to SLAs as per the Contract. The MSP has to provide post implementation support to maintain SLAs. During the O&M, if the Managed Service Provider is unable to comply with the support terms as mentioned in later section, the MSP will have to a pay a penalty as specified under the SLA of this project. Post implementation support would also include support during scheduled DR drills. Managed Service Provider shall perform Disaster Recovery drills once every 6 months .During regular operations while only replication is taking place, in disaster scenario when DR is active and operational, and during switchover and switchback.

2.2 Console Account, Monitoring, Management and Governance: The Managed Service Provider shall have monitoring tools for measuring the utilization of servers, storage, network and security. The tool shall be capable of providing the exact utilization of servers and shall be able to generate per day, per month and per quarter utilization reports based on which the payments will be made. The MSP should also provide access to the portal to BMC DIT and its consultants. The Service Provider should offer a provision for resource inventory, config history and change notifications. The Managed Service Provider should trigger events and alerts on non-conformance on defined governance and should have capability prevent configuration changes. The Managed Service Provider should support installation of 3rd party Application Performance Monitoring agents.

2.3 Disaster Recovery and Backup Services: The Managed Service Provider should provide support on demand for offsite restoration of backup by BMC at no extra cost.

2.4 Upgrades & Software Updates: The Managed Service Provider shall perform patch management appropriate to the scope of their control and/or provide self-service tools to perform patch management. Any required version/Software /Hardware upgrades, patch management etc. at the Cloud Site will be done by the Managed Service Provider for the entire contract period. Application Patch updating will be done by BMC team in co-ordination with Application Vendor System Integration teams .The Managed Service Provider shall document all patch management related activities within the MSP's scope. The Managed Service Provider shall inform BMC for any planned or unplanned activity and also ensure on time alerts are generated well in advance on the upcoming patches via email and management portal.

Communication and collaboration between the department staff and the Managed /Cloud Service Provider's technical support team are vital throughout the defect repair process to ensure timely and effective resolution of issues.

3 Technical Helpdesk Support

Technical support requirements for Cloud Services involve the resources, services, and processes needed to assist users in resolving technical issues and maximizing the system's performance.

The Managed Service Provider shall provide the following key technical support requirements for theCloud Services:

3.1 Help Desk: Establish a help desk or support center staffed with knowledgeable support personnel who can provide assistance to users. The help desk should be accessible through various channels, such as phone, email, live chat or a web-based ticketing system and dedicated support portal, to receive and track user requests for technical support. Adhere to the hours of operation for support services and any exceptions for after-hours or critical issue support, as specified in the contract. CSP / MSP will provide a Single Point of Contact (SPOC) and also escalation/closure of incidents for the IT/User at BMC whose infrastructure is hosted at the cloud site. One dedicated landline/mobile number and email ID shall be provided to BMC. Helpdesk Solution should comprise of a system of raising issues on a portal through web/intranet, call logging, ticket generation, sending alerts on email, and escalation to the cloud administrators and end users.

3.2 Troubleshooting and Issue Resolution: The technical support team should have the expertise to troubleshoot and diagnose technical issues reported by users. They should be able to identify the root causes of problems and provide timely resolutions or workarounds. This may involve remote assistance, guidance on system configuration, software patches, or updates. Provide Help Desk facility during agreed service period window for reporting user incidents/issues/problems with the IT infrastructure. The Help desk shall log user calls related to Cloud Solution and assign an incident/call ID number. Severity shall be assigned to each call as per SLAs. The MSP shall ensure that if any tickets pertain to action from their end, these calls are fully responded by the professional team. Continuous monitoring of the cloud-based IT infrastructure at the site to ensure availability as per SLAs. Escalate the calls, to the appropriate levels, if necessary, as per the escalation matrix agreed between the CSP / MSP and BMC. The escalation matrix shall be developed by the CSP / MSP in discussion with BMC.

3.3 Knowledge Base and Documentation: Maintain a comprehensive knowledge base and documentation repository that contains troubleshooting guides, FAQs, user manuals, and other relevant resources. This enables support personnel to quickly access and share information to assist users in resolving common issues or answering frequently asked questions.

3.4 System Monitoring and Proactive Maintenance: Implement monitoring tools and processes to proactively monitor the performance, availability, and health of the Information System. This helps identify potential issues or system anomalies before they impact users. Regular maintenance activities, such as software updates, database optimizations, and hardware checks, should be performed to ensure the system's stability and performance.

3.5 Training and User Education: Offer training programs and resources to educate users on how to effectively use the Cloud Services.The technical support team should provide guidance on best practices, system usage, and workflows to help users maximize their productivity and minimize potential issues.

3.6 Escalation and Incident Management: Define escalation procedures and service level agreements (SLAs) for handling complex or critical technical issues. Establish clear communication channels and escalation paths to involve higher-level support or engage

with the Managed /Cloud Service Provider's technical experts, if necessary. Incident management processes should be in place to track, prioritize, and manage reported issues throughout their lifecycle.

3.7 System Upgrades and Migration Support: When system upgrades or migrations are required, the technical support team should provide assistance to ensure a smooth transition. This may involve validating system compatibility, performing data migration, coordinating downtime, and conducting post-upgrade testing to verify system functionality.

3.8 Vendor Collaboration and Coordination: Maintain a strong working relationship with the Information System / other support vendor's / OEM's technical support team. This includes regular communication, sharing of system logs or diagnostic information, and collaboration on resolving complex issues or identifying system improvements. The technical support team should act as a liaison between the department users and the Cloud Service Provider to facilitate effective communication and issue resolution.

3.9 Continuous Improvement and Feedback Mechanisms: Implement feedback mechanisms, such as user satisfaction surveys or feedback loops, to gather input from users regarding the technical support services. Analyze user feedback to identify areas of improvement and implement necessary changes to enhance the support experience. Analyze the call statistics. Analyze the incident/call statistics and provide monthly reports including but not limited to:

- Type of incidents/calls logged.
- Incidents/calls resolved.
- Incidents/calls open.
- Email ID/Mobile no.

3.10 24/7 Support Availability: Depending on the BMC department's operational requirements, consider providing 24/7 technical support availability to ensure timely assistance and issue resolution, especially for critical or emergency situations.

The Managed Service Provider shalladhere to the service level agreements (SLAs) specified in the contract that outline the response times, resolution times, and support coverage for different types of technical issues. The technical support requirements should align with the BMC department's needs, budget, and the Managed Service Provider's support capabilities to ensure effective and efficient support services.

H. IMPLEMENTATION SCHEDULE, TERMS OF PAYMENT & SLAS

Following is the implementation schedule alongwith target dates / timelines within which each milestone is required to be completed by the Managed Service Provider. However, the Managed Service Provider may discuss the plan with BMC and any changes required in the plan may be agreed and done mutually.

1. **Implementation Schedule Table**
   - **1.1. Total Project Contract Period is 3 years and 45 days.**
   - **1.2. Completion Period for Provisioning, Migration / Configuration, Testing, Commissioning and Operational Acceptance is 45 days.**
   - **1.3. For Operation and Maintenance (O&M) from the date of Operational Acceptance Date is 3 years.**

The following tables covers consolidated information on Implementation Schedule, Terms of Payment, Service Level Agreements (during Provisioning, Configuration, Testing & Commissioning - PCTC phase), pre-requisites for payment and Liquidated Damages if milestone is not achieved on target date during PCTC phase. Service Level Agreements during Operations & Maintenance (O&M) period are specified separately under clause – Service Level Agreements for Information System during Operations & Maintenance (O&M) phase.

Sr. No	Milestone Description	Timelines	Pre-requisites to be fulfilled for Payment	Payment %	Liquidated Damages
1	Migration, Testing and Go-Live of Existing cloud workload to new CSP.	T+ 45 days	Operational Acceptance Test Certificate Signed by Competent Authority of BMC	100 %	0.40% per week or part thereof, of the total contract cost of for delay beyond T+ 60 days in Operational Acceptance Test.
2	3D GIS migration.	T+ 60 days	Operational Acceptance Test Certificate Signed by Competent Authority of BMC	100 %	0.40% per week or part thereof, of the total contract cost of for delay beyond T+ 60 days in Operational Acceptance Test.
3	Provision of All the security services/ security software and dashboard as mentioned in RFP.	T+ 45 days	Operational Acceptance Test Certificate Signed by Competent Authority of BMC	100 %	0.40% per week or part thereof, of the total contract cost of for delay beyond T+ 60 days in Operational Acceptance Test.
4	Provisioning of SD WAN connectivity for accessing Cloud services.	T+ 45 days	Operational Acceptance Test Certificate Signed by Competent Authority of BMC	100 %	0.40% per week or part thereof, of the total contract cost of for delay beyond T+ 60 days in Operational Acceptance Test.
5	Operations and Maintenance (O&M) from the date of Operational Acceptance Test Charges for Compute, Storage and Services	36 months	after submission of Invoices, Uptime Report, Backup Report, SLA Report/s or any other report as per request etc.	Quarterly Payment	As mentioned in 3. Service Level Agreements for Information System during Operations & Maintenance (O&M) Phase

Price Schedule / Bill of Quantities / Bill of Materials (**PLEASE DO NOT FILL IN COMMERCIAL DETAILS / RATES IN THE FOLLOWING TABLE** - To be filled in the format to be downloaded by the Cloud Service Provider from Mahatender system directly). Table below is only for reference purpose only.

2. Summary of Cost Components (Price Schedules / Bill of Materials & Quantities including terms of payment and SLAs till Operational Acceptance phase)

Sr.No	Item Description	QTY	Unit of Measurement	Total Qty (36Months) (A)
1	Existing Cloud Workload	1	Lumpsum	36
2	LINUX virtual machine (RHEL latest version with Enterprise License support included for the OS) Specification: 4vCPU/8GB RAM/100 GB SSD / 1:2 vCPU/VM (VMs require DC + Cold DR)	22	Number	792
3	Windows virtual machine (Enterprise grade Latest Windows with Enterprise License support included for the OS) Specification: 4vCPU/8GB RAM/100 GB SSD / 1:2 vCPU/VM (VMs require DC + Cold DR)	2	Number	72
4	LINUX virtual machine (RHEL latest version with Enterprise License support included for the OS) Specification: 16vCPU/32GB RAM/100 GB SSD / 1:2 vCPU/VM/16 GB GPU (VMs require DC + Cold DR)	1	Number	36
5	Windows virtual machine (Enterprise grade Latest Windows with Enterprise License support included for the OS) Specification: 16vCPU/32GB RAM/100 GB SSD / 1:2 vCPU/VM/16 GB GPU (VMs require DC + Cold DR)	1	Number	36
6	LINUX virtual machine (Ubantu/RHEL latest version with Enterprise License support included for the OS) Specification: 8vAPU/32GB RAM/250 GB SSD (VMs require DC + Cold DR)	7	Number	252
7	Windows virtual machine (Enterprise grade Latest Windows with Enterprise License support included for the OS) Specification: 8vAPU/32GB RAM/250 GB SSD (VMs require DC + Cold DR)	5	Number	180
8	Additional CPU	245	Number	8820
9	Additional Memory	1500	Number	54000
10	DR Agent (Cloud DC to Cloud DR)	60	Number	2160
11	Additional Block Storage to be attached to VM - SSD High IOPS (5000 IOPS and 200 MB/s throughput per TB) (DC+DR)	125	Number	4500
12	File Share Storage (EFS/NAS) - between multiple virtual machines - SSD	52	Number	1872
13	Backup Agent	60	Number	2160
14	Backup Storage	210	Number	7560

15	Internet Link (500Mbps)	1	Number	36
16	Data Replication (Cloud DC-Cloud DR)	1	12000 GB/month	36
17	SD-WAN solution with necessary licenses and hardware (if any)	1	lumpsum	1
18	SD-WAN link (DC) (Primary link+ secondary link) location (CSP to WDC) (Requirement – 500Mbps)	2	per link/per year	6
19	SD-WAN Link (DR) (Location (DR to WDC) (Requirement –150mbps)	1	per link/per year	3
20	Load Balancer as a service (5 rules)	15	per instance /per month	540
21	Public IP Address	30	Per IP /Month	1080
22	Firewall as a Service (UTM/IPS/IDS)	1	per instance /per month	36
23	Web Application Firewall (vWAF/cWAF) with 10 rules	1	per WAF/per month	36
24	DDOS Protection	1	Lumpsum	1
25	VMDR (Vulnerability Management, Detection, and Response)	1	Lumpsum	1
26	WAS (Web Application Scanning)WAS (Web Application Scanning)	1	Lumpsum	1
27	Threat Vision	1	Lumpsum	1
28	CSPM (Cloud Security Posture Management)	1	Lumpsum	1
29	Wild card SSL Certificate (support unlimited sub-domains)	1	per year	3
30	Micro segmentation Security	1	Lumpsum	1
31	P2P Cross Connect /Termination Charges (DC)	2	per month	72
32	P2P Cross Connect /Termination Charges (DR)	1	per month	36
33	One Time Implementation and Migration Charges	1	Lumpsum	1
34	Migration Charges for 3D GIS	1	Lumpsum	1
35	MSP Charges	1	per month	36

Note: -

- Successful Operational Acceptance Test of each application migrated to the Cloud Service shall be considered as Go-Live.
- Operations & Maintenance period will only start after successful OAT of all the Information Systems migrated to the Cloud Services listed in the above table.
- Payment will be made on actual usage of Services.

2.1 Existing Cloud Workload details :

Sr. No.	Application Group	VM Name	CPUs	RAM	HDD	OS
1	GIS	ESDS-6384-30814-DPGISDEV	4	16	250	Microsoft Windows Server

						2012 (64-bit)
2	GIS	ESDS-6384-36693-Testprsrvgisweb-Restored	4	16	500	RHEL 8.4
3	GIS	ESDS-6384-38826-dpdatabase	8	64	500	Microsoft Windows Server 2012 (64-bit)
4	GIS	ESDS-6384-30815-MUNICIPA32766-Restored-DLU-818-60700	4	32	950	Microsoft Windows Server 2012 (64-bit)
5	GIS	ESDS-6384-30900-GISDEVSERV	4	32	400	Red Hat Enterprise Linux 7 (64-bit)
6	GIS	ESDS-6384-30959-MUNICIPA32769	8	64	950	Microsoft Windows Server 2012 (64-bit)
7	GIS	ESDS-6384-30894-PRSRVGISWEB	4	32	800	Red Hat Enterprise Linux 7 (64-bit)
8	GIS	ESDS-6384-34849-SupportServices	4	32	1150	Ubuntu Linux (64-bit) 20.04.2
9	GIS	ESDS-6384-35330-WEB	4	32	250	Microsoft Windows Server 2016 or later (64-bit)
10	GIS	ESDS-6384-45768-isbmc	4	32	400	Window 2019
11	GIS	ESDS-6384-45766-gisdata	4	32	600	Window 2019
12	GIS	ESDS-6384-34846-PanoramicServer	4	64	1150	Microsoft Window

						s Server 2016 or later (64-bit)
13	AutoDCR	ESDS-6384-36154-AutoDCRDB2	4	64	250	Microsoft Windows Server 2016 or later (64-bit)
14	GIS	ESDS-6384-30896-NAGIOSMONNEW	4	8	290	Red Hat Enterprise Linux 7 (64-bit)
15	CovidSync	ESDS-6384-36825-CovidSync	4	8	500	Microsoft Windows Server 2016 or later (64-bit)
16	GIS	ESDS-6384-35528-WIN	4	8	200	Microsoft Windows Server 2016 or later (64-bit)
17	AutoDCR	ESDS-6384-30871-AUTOCADAPP	4	4	150	Microsoft Windows Server 2012 (64-bit)
18	AutoDCR	ESDS-6384-30859-OMNIAPPSVR01	4	4	500	Red Hat Enterprise Linux 5 (64-bit)
19	AutoDCR	ESDS-6384-30838-OMNIAPPSVR01	4	4	11090	Red Hat Enterprise Linux 5 (64-bit)
20	AutoDCR	ESDS-6384-36152-AutoDCR-DB1	16	64	1250	Microsoft Windows Server

						2016 or later (64-bit)
21	GIS	ESDS-6384-30885-GISPRSRVGISDB	16	64	2900	Red Hat Enterprise Linux 7 (64-bit)
22	PTAX	ESDS-6384-30821-CVSDB1	24	128	5595	Red Hat Enterprise Linux 5 (64-bit)
23	PTAX	ESDS-6384-30846-CVSDB2	24	128	275	Red Hat Enterprise Linux 5 (64-bit)
24	AutoDCR	ESDS-6384-36151-AutoDCR-APP	16	50	38739	Microsoft Windows Server 2016 or later (64-bit)
25	GIS	ESDS-6384-37634-buidprsrvgis_db	16	64	1831	Red Hat Enterprise Linux 8 (64-bit)
26	GIS	CLN-281123-ESDS-6384-36692-Testprsvrgisapp_1-QRF-880-52907	32	14	450	RHEL 8.5
27	GIS	ESDS-6384-55526-prsrvgisapp	16	128	600	RHEL 8.4
28	IPVS	ESDS-6384-40289-WebApp_1	16	64	400	Ubuntu 20.04
29	GIS	ESDS-6384-45767-gismaps	16	32	400	Window 2019
30	GIS	ESDS-6384-56328-buidprsrvgismbapp	32	64	3072	RHEL 8.4
31	AutoDCR	ESDS-6384-36153-AutoDCRAPP2	16	50	9165	Microsoft Windows Server 2016 or later (64-bit)
32	GIS	ESDS-6384-37635-buidprsrvgisapp_1	8	64	504	Red Hat Enterprise Linux 8 (64-bit)

33	GIS	ESDS-6384-36692-Testprsrvgisapp_1	8	64	500	Red Hat Enterprise Linux 8 (64-bit)
34	GIS	ESDS-6384-55525-mumgis	8	64	600	RHEL 8.4
35	GIS	ESDS-6384-55524-mybmcgis	8	64	600	RHEL 8.4
36	GIS	ESDS-6384-30895-PRSRVGISAPP	8	32	520	Red Hat Enterprise Linux 7 (64-bit)
37	CVS	ESDS-6384-30855-DMSERVER	8	32	2024	Red Hat Enterprise Linux 6 (64-bit)
38	GIS	ESDS-6384-37636-buidprsrvgisweb	8	32	650	Red Hat Enterprise Linux 8 (64-bit)
39	GIS	ESDS-6384-45769-web	8	32	600	Window 2019
40	PTAX	ESDS-6384-39668-PRCVS1	36	36	3172	Red Hat Enterprise Linux 5 (64-bit)
41	PTAX	ESDS-6384-39669-PRCVS2	36	36	200	Red Hat Enterprise Linux 5 (64-bit)
42	GIS	ESDS-6384-39667-DPGIS-Restored-DLU-818-60700	16	64	400	Microsoft Windows Server 2012 (64-bit)
43	ABM	ESDS-6384-33387-ABM	12	64	3272	Red Hat Enterprise Linux 5 (64-bit)
44	GIS	ESDS-6384-30960-MUNICIPA32868-Restored-DLU-818-60700	12	64	400	Microsoft Windows Server

						2012 (64-bit)
45	GIS	ESDS-6384-36690-TestPrsrvgisdbP_1	8	16	1831	Red Hat Enterprise Linux 8 (64-bit)
46	AQUA	ESDS-6384-30863-MCGMAQUA02	8	16	405	Red Hat Enterprise Linux 4 (64-bit)
47	GIS	1_1_ESDS-6384-36690-TestPrsrvgisdb-1-Restored-OLD-149-59345	8	16	2855	RHEL 8.4
48	GIS	ESDS-6384-34842-ArcGISPortal-1	12	96	1150	Microsoft Windows Server 2016 or later (64-bit)
49	GIS	ESDS-6384-34843-ArcGISDatastore-1	8	64	1150	Microsoft Windows Server 2016 or later (64-bit)
50	GIS	ESDS-6384-34844-ArcGISServer-1	8	128	1150	Microsoft Windows Server 2016 or later (64-bit)
51	GIS	ESDS-6384-34845-ImageServer1	8	64	1150	Microsoft Windows Server 2016 or later (64-bit)
52	GIS	ESDS-6384-34847-DatabaseServer	18	80	1150	Ubuntu Linux (64-bit) 20.04.2
53	GIS	ESDS-6384-34848-MapDesktop	16	64	3710	Microsoft Windows Server

						2016 or later (64-bit)
54	IPVS	ESDS-6384-40287-DBServer	16	64	400	Ubuntu 20.04
55	IPVS	ESDS-6384-40288-MAPServer_1	16	64	400	Ubuntu 20.04
56	GIS	ESDS-6384-36694-TestIntranetWeb	4	8	431	Red Hat Enterprise Linux 8 (64-bit)
57	GIS	ESDS-6384-36693-Testprsrvgisweb	4	16	431	Red Hat Enterprise Linux 8 (64-bit)
58	GIS	ESDS-6384-36691-Testgisdevserv1	4	16	400	Red Hat Enterprise Linux 8 (64-bit)
59	GIS	ESDS-6384-6474-agsmaps2	16	32	600	Windows Server 2019 STD.
60	GIS	ESDS-6384-64740-dpgisdevq	16	32	700	Windows Server 2019 STD.
61	#N/A	#N/A				#N/A
62	Tenements	ESDS-6384-69320-WIN	8	32	100	Windows Server 2022
63	Tenements	ESDS-6384-69311-LIN	8	16	100	Ubuntu 22.04
64	GIS	ESDS-6384-69337-agsmaps3	16	64	500	Windows Server 2019
65	GIS	ESDS-6384-69330-dpgisportal	8	64	3200	Windows Server 2019
66	GIS	ESDS-6384-69329-dpdocs	4	32	4100	Windows Server 2019

3. Service Level Agreements for Information System during Operations & Maintenance (O&M) Phase

A Service Level Agreement (SLA) for Information System outlines the agreed-upon levels of service and performance between the Managed Service Provider of Information System and the BMC. The Managed Service Provider shall fulfill following SLAs regarding system availability, response times, support, and other key metrics during O&M Phase of the project.

#	Service Level Objective	Definition	Target	Penalty
Availability				
1	Availability of each cloud service(Applicable for all Cloud Service)	Availability means, the aggregate number of hours in a calendar month during which cloud service is actually available for use Uptime Calculation for the calendar month: {[(Uptime Hours in the calendar month + Scheduled Downtime in the calendar month) / Total No. of Hours in the calendar month] x 100}	Availability for Compute and Storage Services >= 99.9%	Penalty as indicated below(per occurrence): a) <99.9%to>=99.00%-10%of Quarterly Payment of bidder/SI/MSP b) <99.00%to>=98.50%-15%of Quarterly Payment of bidder/SI/MSP c) <98.50%to>=98.00%-20%of Quarterly Payment of bidder/SI/MSP . <98%-30%oftheQuarterly Quarterly Payment of bidder/SI/MSP In case the services are not available for a continuous period of 8 Business Hours on any day, penalty shall be 100% of the Quarterly Payment due to the cloud service provider.
2	Availability of regular reports (SLA, Cloud Services Consumption, Monitoring, Security)	Regular reports should be submitted to BMC within5workingdaysfrom the end of the month.	Regular reports should be submitted to BMC within5workingdaysfrom the end of the service month	Penalty as indicated below(per occurrence): <11 working days to >= 6 workingdays-5%of Quarterly Payment of bidder/SI/MSP <16 working days to >= 10 workingdays-10% Quarterly Payment of bidder/SI/MSP . For the delay beyond 15days, penalty of 15% of the Quarterly Payment of bidder/SI/MSP and increasing by 1% with each passing day
Performance				

3	Provisioning and de-provisioning of Virtual Machine	Time to provision/de-provision virtual Machine Measurement shall be done on the basis of ticket resolution	Each time within4 hours	INR 5000 on each occurrence, INR 1000 for delay of every hour beyond 4 hours.
4	Provision/De-provision additional resources	Time to provision additional APU/vCPU/vRAM/Storage etc. Measurement shall be done on the basis of ticket resolution	Each time within4 hours	INR 5000 on each occurrence, INR 2000 for delay of every hour beyond 4 hours.
5	Utilization metrics for all Cloud Services	The usage details for all the Cloud Service	Should be available within 1 hour of actual usage. .	INR 2500 on each occurrence, INR 1000 for delay of every hour beyond 4 hours.
		Security		
6	Percentage of timely vulnerability reports	Percentage of timely vulnerability reports shared by the CSP/MSP Occurrence Quarterly.	Should be shared with BMC within 15 working days of vulnerability identification	INR 2500 on each occurrence, INR 1000 for delay of every 1 day beyond 15 days.
7	Percentage of timely vulnerability corrections	Percentage of timely vulnerability corrections performed by the Cloud Service Provider. a) High Severity - Perform vulnerabilitycorrectionwithin 30 days of vulnerability identification. b) Medium Severity - Perform vulnerabilitycorrectionwithin 60 days of vulnerability identification. c) Low Severity - Perform vulnerabilitycorrectionwithin 90 days of vulnerability identification. Measurement period is calendar month.	Percentage of timely vulnerability corrections performed by the Cloud Service Provider. d) High Severity - Perform vulnerabilitycorrectionwit hin30 days of vulnerability identification. e) Medium Severity - Perform vulnerabilitycorrectionwit hin60 days of vulnerability identification. f) Low Severity - Perform vulnerabilitycorrectionwit hin90 days of vulnerability identification. Measurement period is calendar month.	Penalty as indicated below(per occurrence): a) <99.5%to>=99.00%-10%of Quarterly Payment of bidder/SI/MSP b) <99.00%to>=98.00%-20%of Quarterly Payment of bidder/SI/MSP c)<98%-30%ofQuarterly Quarterly Payment of bidder/SI/MSP .
8	Security breach including Data Theft/Loss/Corruption	Any incident wherein system including all cloud-based services and components are compromised or any case wherein data theft occurs.	No breach	For each breach/data theft, penalty will be levied as per following criteria. 1. Severity1 (as define in Annexure A) - Penalty of Rs 15 Lakh per incident. 2. Severity2 (as define in Annexure A) - Penalty of Rs 10 Lakh per incident. 3. Severity3 (as define in Annexure A) - Penalty of Rs 5 Lakh per incident.

				These penalties will not be part of overall SLA penalties cap per month. In case of serious breach of security wherein the data is stolen or corrupted, BMC reserves the right to terminate the contract.
9	Security Incident (Malware Attack/Denial of Service Attack/ Data Theft/ Loss of data/ Intrusion or Defacement) Applicable on the CSP's underlying infrastructure	Security incidents could consist of any of the following: Malware Attack :This shall include Malicious code infection of any of the resources, including physical and virtual infrastructure and applications. Denial of Service Attack: This shall include non-availability of any of the Cloud Service due to attacks that consume related resources .The Service Provider shall be responsible for monitoring, detecting and resolving all Denial of Service (DoS) attacks. Intrusion: Successful unauthorized access to system, resulting in loss of confidentiality / Integrity/availability of data. The Service Provider shall be responsible for monitoring, detecting and resolving all security related intrusions on the network using an Intrusion Prevention device.	a) Any Denial -of-service attack shall not lead to complete service non- availability. b) Zero Malware attack/ Denial of Service attack/ Intrusion / Data Theft	For each occurrence of any of the attacks (Malware attack/Denial of Service attack / Intrusion / Data Theft), 25% of the Quarterly Payment due to the cloud service provider..
Support Channels–Incident / Request and Help desk				
10	Response Time/Acknowledgement for Helpdesk ticket	Average Time taken to acknowledge and respond, once a ticket/incident is logged through one of the agreed channels.	For all incidents, should be acknowledged within 15 minutes of ticket raised	>15 min INR 2500 on every un-responded call and subsequently additional INR 1000 on every hour on For the same.

11	Time to Resolve - Severity 1	Time taken to resolve the reported ticket/incident from the time of logging.	For Severity 1 incidents, should be resolved within 1 hour of reporting	>1 hour INR 5000 on every unresolved call and subsequently additional INR 2500 on every hour on Un-resolved call.
12	Time to Resolve - Severity 2	Time taken to resolve the reported ticket/incident from the time of logging.	For Severity 2 incidents, should be resolved within 2.5 hours of reporting	>2.5 hours INR 3000 on every unresolved call and subsequently additional INR 1500 on every hour on Un-resolved call.
13	Time to Resolve - Severity 3	Time taken to resolve the reported ticket/incident from the time of logging.	For Severity 3 incidents, should be resolved within 8 hours of reporting	>8 hours INR 1000 on every unresolved call and subsequently additional INR 500 on every hour on Un-resolved call.
14	Time to Resolve - Severity 4	Time taken to resolve the reported ticket /incident from the time of logging.	For Severity 4 incidents, should be resolved within 24 hours of reporting	>24 hours INR 500 on every unresolved call and subsequently additional INR 500 on every hour on Un-resolved call.
Disaster Recovery and Data Back up Management				
15	Recovery Time Objective (RTO) (Applicable during Disaster Recovery)	Measured during the regular planned or unplanned (outage) change over from DC to DR or vice versa.	RTO<=2 hours	10% of Quarterly Payment of bidder/SI/MSP per every additional 2(two) hours of downtime
16	RPO (Applicable when taking Disaster Recovery as a Service from the Service Provider)	Measured during the regular planned or unplanned (outage) change over from DC to DR or vice versa.	RPO<=1hour Transactional and Critical Data -15 minutes Applications and OS - 60 minutes	10% of Quarterly Payment of bidder/SI/MSP additional 2(two) hours of data loss

17	DR Drills	As and when requested by BMC.	MSP and CSP has to submit plan for DR drill within 7 working days after request raised by BMC. And DR drill to be conducted as per date given by BMC	a) 50,000/- for each request raised for each application deployed
Audit& Compliance				
18	Patch Application	Patch updates to underlying infrastructure and cloud service Measurement shall be done by analyzing security audit reports	Within 2 hour after request raise by BMC.	Penalty as indicated below (per occurrence): a) <95%to>=90.00%-5%of Quarterly Payment of bidder/SI/MSP b) <90%to>=85.0%-10%of Quarterly Payment of bidder/SI/MSP c) <85%to>=80.0%-15%of Quarterly of bidder/SI/MSP d) <80%- 20%of the Quarterly Payment of bidder/SI/MSP.

The Helpdesk support/Issue resolution of the Managed Service Provider should offer the below mentioned level

The Service Level Agreement (SLA) for Helpdesk support/issues/tickets resolution outlines the agreed-upon levels of service and performance between the Managed Service Provider and the BMC. The Supplier shall fulfill following SLAs:
*Call mentioned above can be any method of raising ticket i.e. phone call, ticket through portal, email or chat

Annexure A - Severity Levels

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

Severity Level	Description	Examples
Severity 1	Environment is down or major malfunction resulting in an 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	Non-availability of VM. connectivity No access to Storage, software or application No access to cloud workload due to network unavailability.

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.	Intermittent network connectivity
Severity 3	Moderate loss of performance resulting in multiple users (includes public users) impacted in their normal functions.	Not impacting operations immediately but may impact services if not attended
Severity 4	No impact on delivery but issues like improvement suggestions etc or questions	An error in software product Documentation

**Note: - Any additional request from BMC may specify the priority /severity in the ticket detail.

Section VI - General Conditions of Contract

A. CONTRACT AND INTERPRETATION

1. Definitions

a. In this Contract, the following terms shall be interpreted as indicated below.

i) contract elements

(1) "Contract" means the Contract Agreement entered into between BMC and the Managed Service Provider, together with the Contract Documents referred to therein. The Contract Agreement and the Contract Documents shall constitute the Contract, and the term "the Contract" shall in all such documents be construed accordingly.

(2) "Contract Documents" means the documents specified in Article 1.1 (Contract Documents) of the Contract Agreement (including any amendments to these Documents).

(3) "Contract Agreement" means the agreement entered into between BMC and the Managed Service Provider using the form of Contract Agreement contained in the Sample Contractual Forms Section of the bidding documents and any modifications to this form agreed to by BMC and the Cloud Service Provider. The date of the Contract Agreement shall be recorded in the signed form.

(4) "GCC" means the General Conditions of Contract.

(5) "SCC" means the Special Conditions of Contract.

(6) "Technical Requirements" means the Section - Technical Requirements in the bidding documents.

(7) "Implementation Schedule" means the Section - Implementation Schedule in the bidding documents.

(8) "Contract Price" means the price or prices defined in Article 2 (Contract Price and Terms of Payment) of the Contract Agreement.

(9) "Bidding documents" refers to the collection of documents issued by BMC to instruct and inform potential Managed Service Providers of the processes for bidding, selection of the winning bid, and Contract formation, as well as the contractual conditions governing the relationship between BMC and the Managed Service Provider. The General and Special Conditions of Contract, the Technical Requirements, and all other documents included in the bidding documents reflect the Procurement Regulations that BMC is

obligated to follow during procurement and administration of this Contract.

ii) entities

(1) "Purchaser" means the entity purchasing the Cloud Services, which is Brihanmumbai Municipal Corporation (BMC).

(2) "Project Manager" means the personappointed by BMC in the manner provided in GCC Clause (Representatives - Project Manager) to perform the duties delegated by BMC.

(3) "Managed Service Provider" means the firm or Joint Venture whose bid to perform the Contract has been accepted by BMC and is named as such in the Contract Agreement.

(4) "Managed / Cloud Service Provider's Representative" means any person nominated by the Managed / Cloud Service Provider and named as such in the Contract Agreement or otherwise approved by BMC in the manner provided in GCC Clause (Representatives - Managed Service Provider's Representative) to perform the duties delegated by the Cloud Service Provider.

(5) "Subcontractor" means any firm to whom any of the obligations of the Managed /Cloud Service Provider, including preparation of any design or supply of any Information Technologies or other Goods or Services, is subcontracted directly or indirectly by the Managed / Cloud Service Provider.

(6) "Adjudicator" means the person named in Appendix 2 of the Contract Agreement, appointed by agreement between BMC and the Cloud Service Provider to make a decision on or to settle any dispute between BMC and the Managed / Cloud Service Provider referred to him or her by the parties, pursuant to GCC Clause (Adjudication).

iii) scope

(1) "Cloud Services" means a wide range of services including but not limited to infrastructure, platforms, software, and other services that can be quickly provisioned and scaled to meet the needs of users, hosted on remote servers in data centers and delivered over the internet and / or intranet that provide various types of computing resources without the need for local infrastructure.

(2) "Information System," also called "the System," means all the Information Technologies, Materials, and other Goods to be supplied, installed, integrated, and made operational (exclusive of the Cloud Service Provider's Equipment), together with the Services to be carried out by the Cloud Service Provider under the Contract.

(3) "Subsystem" means any subset of the System identified as such in the Contract that may be supplied, installed, tested, and commissioned individually before Commissioning of the entire System.

(4) "Information Technologies" means all information processing and communications-related hardware, Software, supplies, and consumable items that the Cloud Service Provider is required to supply and install under the Contract.

(5) "Goods" means all equipment, machinery, furnishings, Materials, and other tangible items that the Cloud Service Provider is required to supply or supply and install under the Contract, including, without limitation, the Information Technologies and Materials, but excluding the Cloud Service Provider's Equipment.

(6) "Services" means all technical, logistical, management, and any other Services to be provided by the Cloud Service Provider under the Contract to supply, install, customize, integrate, and make operational the System. Such Services may include, but are not restricted to, activity management and quality assurance, design, documentation, transportation, insurance, inspection, expediting, site

preparation, installation, integration, training, data migration, Pre-commissioning, Commissioning, maintenance, and technical support.

(7) "The Project Plan" means the document to be developed by the Cloud Service Provider and approved by BMC, pursuant to GCC Clause (Project Plan), based on the requirements of the Contract and the Preliminary Project Plan included in the Cloud Service Provider's bid. The "Agreed Project Plan" is the version of the Project Plan approved by BMC, in accordance with GCC Clause (Project Plan). Should the Project Plan conflict with the Contract in any way, the relevant provisions of the Contract, including any amendments, shall prevail.

(8) "Software" means that part of the System which are instructions that cause information processing Subsystems to perform in a specific manner or execute specific operations.

(9) "System Software" means Software that provides the operating and management instructions for the underlying hardware and other components, and is identified as such in Appendix 4 of the Contract Agreement and such other Software as the parties may agree in writing to be Systems Software. Such System Software includes, but is not restricted to, micro-code embedded in hardware (i.e., "firmware"), operating systems, communications, system and network management, and utility software.

(10) "General-Purpose Software" means Software that supports general-purpose office activities and is identified as such in Appendix 4 of the Contract Agreement and such other Software as the parties may agree in writing to be General- Purpose Software. Such General-Purpose Software may include, but is not restricted to, word processing, spreadsheet, generic database management, and application development software.

(11) "Application Software" means Software formulated to perform specific business or technical functions and interface with the business or technical users of the System and is identified as such in Appendix 4 of the Contract Agreement and such other Software as the parties may agree in writing to be Application Software.

(12) "Standard Software" means Software identified as such in Appendix 4 of the Contract Agreement and such other Software as the parties may agree in writing to be Standard Software.

(13) "Custom Software" means Software identified as such in Appendix 4 of the Contract Agreement and such other Software as the parties may agree in writing to be Custom Software.

(14) "Source Code" means the database structures, dictionaries, definitions, program source files, and any other symbolic representations necessary for the compilation, execution, and subsequent maintenance of the Software (typically, but not exclusively, required for Custom Software).

(15) "Materials" means all documentation in printed or printable form and all instructional and informational aides in any form (including audio, video, and text) and on any medium, provided to BMC under the Contract.

(16) "Standard Materials" means all Materials not specified as Custom Materials.

(17) "Custom Materials" means Materials developed by the Cloud Service Provider at BMC's expense under the Contract and identified as such in Appendix 5 of the Contract Agreement and such other Materials as the parties may agree in writing to be Custom Materials. Custom Materials includes Materials created from Standard Materials.

(18) "Intellectual Property Rights" means any and all copyright, moral rights, trademark, patent, and other intellectual and proprietary rights, title and interests worldwide, whether vested, contingent, or future,

including without limitation all economic rights and all exclusive rights to reproduce, fix, adapt, modify, translate, create derivative works from, extract or re-utilize data from, manufacture, introduce into circulation, publish, distribute, sell, license, sublicense, transfer, rent, lease, transmit or provide access electronically, broadcast, display, enter into computer memory, or otherwise use any portion or copy, in whole or in part, in any form, directly or indirectly, or to authorize or assign others to do so.

(19) "Managed / Cloud Service Provider's Equipment" means all equipment, tools, apparatus, or things of every kind required in or for installation, completion and maintenance of the System that are to be provided by the Managed / Cloud Service Provider, but excluding the Information Technologies, or other items forming part of the System.

iv) activities

(1) "Delivery" means the transfer of the Goods from the Cloud Service Provider to BMC in accordance with the current edition Incoterms specified in the Contract.

(2) "Installation" means that the System or a Subsystem as specified in the Contract is ready for Commissioning as provided in GCC Clause (Installation of the System).

(3) "Pre-commissioning" means the testing, checking, and any other required activity that may be specified in the Technical Requirements that are to be carried out by the Cloud Service Provider in preparation for Commissioning of the System as provided in GCC Clause (Installation of the System).

(4) "Commissioning" means operation of the System or any Subsystem by the Cloud Service Provider following Installation, which operation is to be carried out by the Cloud Service Provider as provided in GCC Clause (Commissioning and Operational Acceptance), for the purpose of carrying out Operational Acceptance Test(s).

(5) "Operational Acceptance Tests" means the tests specified in the Technical Requirements and Agreed Project Plan to be carried out to ascertain whether the System, or a specified Subsystem, is able to attain the functional and performance requirements specified in the Technical Requirements and Agreed Project Plan, in accordance with the provisions of GCC Clause (Commissioning and Operational Acceptance).

(6) "Operational Acceptance" means the acceptance by BMC of the System (or any Subsystem(s) where the Contract provides for acceptance of the System in parts), in accordance with GCC Clause (Commissioning and Operational Acceptance).

v) place and time

(1) "Managed / Cloud Service Provider's Country" is the country in which the Cloud Service Provider is legally organized, as named in the Contract Agreement.

(2) "Project Site(s)" means the place(s) in the Site Table in the Technical Requirements Section for the supply and installation of the System.

(3) "Day" means calendar day of the Gregorian Calendar.

(4) "Week" means seven (7) consecutive Days, beginning the day of the week i.e. Monday as is customary in India.

(5) "Month" means calendar month of the Gregorian Calendar.

(6) "Year" means twelve (12) consecutive Months.

(7) "Effective Date" means the date of fulfillment of all conditions specified in Article 3 (Effective Date for Determining Time for Achieving Operational Acceptance) of the Contract Agreement, for the purpose of determining the Delivery, Installation, and Operational Acceptance dates for the System or Subsystem(s).

(8) "Contract Period" is the time period during which this Contract governs the relations and obligations of BMC and Cloud Service

Provider in relation to the System, the Contract shall continue in force until the Cloud Services have been provided, unless the Contract is terminated earlier in accordance with the terms set out in the Contract.

(9) "Defect Liability Period" (also referred to as the "Warranty Period") means the period of validity of the warranties given by the Cloud Service Provider commencing at date of the Operational Acceptance Certificate of the System or Subsystem(s), during which the Cloud Service Provider is responsible for defects with respect to the System (or the relevant Subsystem[s]) as provided in GCC Clause (Defect Liability).

(10) "The Coverage Period" means the Days of the Week and the hours of those Days during which maintenance, operational, and/or technical support services (if any) must be available.

(11) "The Post-Warranty Services Period" means the number of years defined in the Section – BMC's Requirements (if any), following the expiration of the Warranty Period during which the Cloud Service Provider may be obligated to provide Software licenses, maintenance, and/or technical support services for the System, either under this Contract or under separate contract(s).

2. Contract Documents

a. Subject to Article 1.2 (Order of Precedence) of the Contract Agreement, all documents forming part of the Contract (and all parts of these documents) are intended to be correlative, complementary, and mutually explanatory. The Contract shall be read as a whole.

3. Interpretation

a. Governing Language

i. All Contract Documents and related correspondence exchanged between BMC and Cloud Service Provider shall be written in the language of these bidding documents (English), and the Contract shall be construed and interpreted in accordance with that language.

ii. If any of the Contract Documents or related correspondence are prepared in a language other than the governing language under GCC Clause above, the translation of such documents into the governing language shall prevail in matters of interpretation. The originating party, with respect to such documents shall bear the costs and risks of such translation.

b. Singular and Plural
The singular shall include the plural and the plural the singular, except where the context otherwise requires.

c. Headings
The headings and marginal notes in the GCC are included for ease of reference and shall neither constitute a part of the Contract nor affect its interpretation.

d. Persons
Words importing persons or parties shall include firms, corporations, and government entities.

e. Incoterms
Unless inconsistent with any provision of the Contract, the meaning of any trade term and the rights and obligations of parties thereunder shall be as prescribed by the Incoterms. Incoterms means international rules for interpreting trade terms published by the International Chamber of Commerce (latest edition), 38 Cours Albert 1er, 75008 Paris, France.

f. Entire Agreement
The Contract constitutes the entire agreement between BMC and Cloud Service Provider with respect to the subject matter of Contract and supersedes allcommunications, negotiations, and agreements (whether written or oral) ofparties with respect to the subject matter of the Contract made prior to thedate of Contract.

g. Amendment
No amendment or other variation of the Contract shall be effective unless it is in writing, is dated, expressly refers to the Contract, and is signed by a duly authorized representative of each party to the Contract.

h. Independent Managed / Cloud Service Provider

The Managed / Cloud Service Provider shall be an independent contractor performing the Contract. The Contract does not create any agency, partnership, joint venture, or other joint relationship between the parties to the Contract. Subject to the provisions of the Contract, the Cloud Service Provider shall be solely responsible for the manner in which the Contract is performed. All employees, representatives, or Subcontractors engaged by the Cloud Service Provider in connection with the performance of the Contract shall be under the complete control of the Cloud Service Provider and shall not be deemed to be employees of BMC, and nothing contained in the Contract or in any subcontract awarded by the Cloud Service Provider shall be construed to create any contractual relationship between any such employees, representatives, or Subcontractors and BMC.

i. Joint Venture
If the Managed / Cloud Service Provider is a Joint Venture of two or more firms, all such firms shall be jointly and severally bound to BMC for the fulfillment of the provisions of the Contract and shall designate one of such firms to act as a leader with authority to bind the Joint Venture. The composition or constitution of the Joint Venture shall not be altered without the prior consent of BMC.

j. Nonwaiver
    i. Subject to GCC Clause below, no relaxation, forbearance, delay, or indulgence by either party in enforcing any of the terms and conditions of the Contract or the granting of time by either party to the other shall prejudice, affect, or restrict the rights of that party under the Contract, nor shall any waiver by either party of any breach of Contract operate as waiver of any subsequent or continuing breach of Contract.
    ii. Any waiver of a party's rights, powers, or remedies under the Contract must be in writing, must be dated and signed by an authorized representative of the party granting such waiver, and must specify the right and the extent to which it is being waived.
    iii. Severability If any provision or condition of the Contract is prohibited or rendered invalid or unenforceable, such prohibition, invalidity, or unenforceability shall not affect the validity or enforceability of any other provisions and conditions of the Contract.

k. Country of Origin

"Origin" means the place where the Information Technologies, Materials, and other Goods for the System were produced or from which the Services are supplied. Goods are produced when, through manufacturing, processing, Software development, or substantial and major assembly or integration of components, a commercially recognized product results that is substantially different in basic characteristics or in purpose or utility from its components. The Origin of Goods and Services is distinct from the nationality of the Cloud Service Provider and may be different.

4. Notices

a. Unless otherwise stated in the Contract, all notices to be given under the Contract shall be in writing and shall be sent, pursuant to GCC Clause below, by personal delivery, airmail post, special courier, facsimile, electronic mail, or Electronic Data Interchange (EDI), with the following provisions.
    i. Any notice sent by facsimile, electronic mail, or EDI shall be confirmed within two (2) days after dispatch by notice sent by airmail post or special courier, except as otherwise specified in the Contract.

ii. Any notice sent by airmail post or special courier shall be deemed (in the absence of evidence of earlier receipt) to have been delivered ten (10) days after dispatch. In proving the fact of dispatch, it shall be sufficient to show that the envelope containing such notice was properly addressed, stamped, and conveyed to the postal authorities or courier service for transmission by airmail or special courier.
iii. Any notice delivered personally or sent by facsimile, electronic mail, or EDI shall be deemed to have been delivered on the date of its dispatch.
iv. Either party may change its postal, facsimile, electronic mail, or EDI addresses for receipt of such notices by ten (10) days' notice to the other party in writing.

b. Notices shall be deemed to include any approvals, consents, instructions, orders, certificates, information and other communication to be given under the Contract.
c. Pursuant to GCC Clause (Representatives), notices from/to BMC are normally given by, or addressed to, the Project Manager, while notices from/to the Managed / Cloud Service Provider are normally given by, or addressed to, the Managed / Cloud Service Provider's Representative, or in its absence its deputy if any. If there is no appointed Project Manager or Managed / Cloud Service Provider's Representative (or deputy), or for any other reason, BMC or Managed / Cloud Service Provider may give and receive notices at their fallback addresses. The address of the Project Manager and the fallback address of BMC are as subsequently established/amended. The address of the Cloud Service Provider's Representative and the fallback address of the Managed / Cloud Service Provider are as specified in Appendix 1 of the Contract Agreement or as subsequently established/amended.

5. Governing Law

a. The Contract shall be governed by and interpreted in accordance with the laws of India.

b. Throughout the execution of the Contract, the Managed / Cloud Service Provider shall comply with the import of goods and services prohibitions in India when

i. as a matter of law or official regulations, India prohibits commercial relations with that country; or

ii. by an act of compliance with a decision of the United Nations Security Council taken under Chapter VII of the Charter of the United Nations, India prohibits any import of goods from that country or any payments to any country, person, or entity in that country.

6. Fraud and Corruption

a. BMC requires compliance with the BMC's Anti-Corruption Guidelines and its prevailing sanctions policies and procedures (as detailed in Section VI – Fraud and Corruption)

b. BMC requires the Managed / Cloud Service Provider 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 bidding 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.

B. SUBJECT MATTER OF CONTRACT

7. Scope of the System

a. The Managed / Cloud Service Provider's obligations cover the provision of all Information Technologies, Materials and other Goods as well as the performance of all Services required for the design, configuration, and implementation (including procurement, quality assurance, assembly, associated site preparation, Delivery, Pre-commissioning, Installation, Testing, and Commissioning) of the System, in

accordance with the plans, procedures, specifications, drawings, codes, and any other documents specified in the Contract and the Agreed Project Plan.

b. The Managed / Cloud Service Provider shall, unless specifically excluded in the Contract, perform all such work and / or supply all such items and Materials not specifically mentioned in the Contract but that can be reasonably inferred from the Contract as being required for attaining Operational Acceptance of the System as if such work and / or items and Materials were expressly mentioned in the Contract.

c. The Managed / Cloud Service Provider's obligations (if any) to provide Goods and Services as implied by the Recurrent Cost tables of the Cloud Service Provider's bid, such as consumables, spare parts, and technical services (e.g., maintenance, technical assistance, and operational support), are as specified in the Section – BMC's Requirements, including the relevant terms, characteristics, and timings.

8. Time for Commencement and Operational Acceptance

a. The Managed / Cloud Service Provider shall commence work on the System within the period specified in the Implementation Schedule under Section – BMC's Requirements, and without prejudice to GCC Clause (Operational Acceptance Time Guarantee), the Cloud Service Provider shall thereafter proceed with the System in accordance with the time schedule specified in the Implementation Schedule and any refinements made in the Agreed Project Plan.

b. The Managed / Cloud Service Provider shall achieve Operational Acceptance of the System (or Subsystem(s) where a separate time for Operational Acceptance of such Subsystem(s) is specified in the Contract) in accordance with the time schedule specified in the Implementation Schedule and any refinements made in the Agreed Project Plan, or within such extended time to which the Cloud Service Provider shall be entitled under GCC Clause (Extension of Time for Achieving Operational Acceptance).

9. Managed / Cloud Service Provider's Responsibilities

a. The Managed / Cloud Service Provider shall conduct all activities with due care and diligence, in accordance with the Contract and with the skill and care expected of a competent provider of information technologies, Cloud Services, support, maintenance, training, and other related services, or in accordance with best industry practices. In particular, the Managed / Cloud Service Provider 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.

b. The Managed / Cloud Service Provider confirms that it has entered into this Contract on the basis of a proper examination of the data relating to the System provided by BMC and on the basis of information that the Managed / Cloud Service Provider could have obtained from a visual inspection of the site (if access to the site was available) and of other data readily available to the Managed / Cloud Service Provider relating to the System as at the date thirty (30) days prior to bid submission. The Managed / Cloud Service Provider 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.

c. The Managed / Cloud Service Provider shall be responsible for timely provision of all resources, information, and decision making under its control that are necessary to reach a mutually Agreed Project Plan (pursuant to GCC Clause (Project Plan) within the time schedule specified in the Implementation Schedule. Failure to provide such resources, information, and decision-making may constitute grounds for termination pursuant to GCC Clause (Termination).

d. The Managed / Cloud Service Provider shall acquire in its name all permits, approvals, and/or licenses from all local, state, or national government authorities or public service undertakings in India that are necessary for the performance of the

Contract, including, without limitation, visas for the Cloud Service Provider's and Subcontractor's personnel and entry permits for all imported Cloud Service Provider's Equipment. The Managed / Cloud Service Provider shall acquire all other permits, approvals, and/or licenses that are not the responsibility of BMC under GCC Clause (BMC's Responsibility) and that are necessary for the performance of the Contract.

e. The Managed / Cloud Service Provider 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 Cloud Service Provider. The Managed / Cloud Service Provider shall indemnify and hold harmless BMC 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 Managed / Cloud Service Provider or its personnel, including the Subcontractors and their personnel, but without prejudice to GCC Clause (BMC's Responsibilities). The Managed / Cloud Service Provider shall not indemnify BMC to the extent that such liability, damage, claims, fines, penalties, and expenses were caused or contributed to by a fault of BMC.

~~f.~~ The Managed / Cloud Service Provider shall, in all dealings with its labor and the labor of its Subcontractors currently employed on or connected with the Contract, pay due regard to all recognized festivals, official holidays, religious or other customs, and all local laws and regulations pertaining to the employment of labor.

~~g.~~ Any Information Technologies or other Goods and Services that will be incorporated in or be required for the System and other supplies shall have their Origin, as defined in GCC Clause (Interpretation)

10. BMC's Responsibilities

a. BMC shall ensure the accuracy of all information and/or data to be supplied by BMC to the Cloud Service Provider, except when otherwise expressly stated in the Contract.

b. BMC shall be responsible for timely provision of all resources, information, and decision making under its control that are necessary to reach an Agreed Project Plan (pursuant to GCC Clause (Project Plan)) within the time schedule specified in the Implementation Schedule. Failure to provide such resources, information, and decision making may constitute grounds for Termination pursuant to GCC Clause (Termination).

c. BMC shall be responsible for acquiring and providing legal and physical possession of the site and access to it, and for providing possession of and access to all other areas reasonably required for the proper execution of the Contract.

d. If requested by the Cloud Service Provider, BMC shall use its best endeavors to assist the Managed / Cloud Service Provider 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 Managed / Cloud Service Provider or Subcontractors or the personnel of the Managed / Cloud Service Provider or Subcontractors, as the case may be, to obtain.

e. In such cases where the responsibilities of specifying and acquiring or upgrading telecommunications and/or electric power services falls to the Cloud Service Provider, as specified in the Technical Requirements, Agreed Project Plan, or other parts of the Contract, BMC shall use its best endeavors to assist the Managed / Cloud Service Provider in obtaining such services in a timely and expeditious manner.

f. BMC 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 Project Plan, except where provision of such items is explicitly identified in the Contract as being the responsibility of the Cloud Service Provider. Delay by BMC may result in an appropriate extension of the Time for Operational Acceptance.

g. Unless otherwise specified in the Contract or agreed upon by BMC and the Cloud Service Provider, BMC shall provide sufficient, properly qualified operating and technical personnel, as required by the Managed / Cloud Service Provider to properly carry out Delivery, Pre-commissioning, Installation, Commissioning, and Operational Acceptance, at or before the time specified in the Implementation Schedule and the Agreed Project Plan.

h. BMC will designate appropriate staff for the training courses to be given by the Managed / Cloud Service Provider and shall make all appropriate logistical arrangements for such training as specified in the Technical Requirements, the Agreed Project Plan, or other parts of the Contract.

i. BMC assumes primary responsibility for the Operational Acceptance Test(s) for the System, in accordance with GCC Clause (Commissioning and Operational Acceptance), and shall be responsible for the continued operation of the System after Operational Acceptance. However, this shall not limit in any way the Cloud Service Provider's responsibilities after the date of Operational Acceptance otherwise specified in the Contract.

j. BMC is responsible for performing and safely storing timely and regular backups of its data and Software in accordance with accepted data management principles, except where such responsibility is clearly assigned to the Managed / Cloud Service Provider elsewhere in the Contract.

k. All costs and expenses involved in the performance of the obligations under this GCC Clause (BMC's Responsibilities) shall be the responsibility of BMC, save those to be incurred by the Managed / Cloud Service Provider with respect to the performance of the Operational Acceptance Test(s), in accordance with GCC Clause (Commissioning and Operational Acceptance).

l. BMC shall have no other Purchaser's responsibilities.

C. PAYMENT

11. Contract Price

a. The Contract Price shall be as specified in Article 2 (Contract Price and Terms of Payment) of the Contract Agreement.

b. The Contract Price shall be a firm lump sum not subject to any alteration, except in the event of a Change in the System pursuant to GCC Clause (Changes to the System) or to other clauses in the Contract;

c. The Managed / Cloud Service Provider 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.

12. **Terms of Payment**

a. The Cloud Service Provider's request for payment shall be made to BMC in writing, accompanied by an invoice describing, as appropriate, the System or Subsystem(s), Delivered, Pre-commissioned, Installed, and Operationally Accepted, and by documents submitted pursuant to GCC Clause (Procurement, Delivery, and Transport) and upon fulfillment of other obligations stipulated in the Contract. **The Contract Price shall be paid as specified in the relevant section of Section – BMC's Requirements.**

b. No payment made by BMC herein shall be deemed to constitute acceptance by BMC of the System or any Subsystem(s).

~~c.~~ Payments shall be made by BMC, after submission of a valid invoice by the Cloud Service Provider.

d. Payments shall be made in the currency(ies) specified in the Contract Agreement, pursuant to GCC Clause (BMC's Responsibilities). For Goods and Services supplied locally, payments shall be made in Indian Rupees (INR).

13. Securities

a. Issuance of Securities

The Managed / Cloud Service Provider shall provide the securities specified below in favor of BMC at the times and in the amount, manner, and form specified below.

b. Performance Security

i. The Managed / Cloud Service Provider shall, within thirty (30) days of the notification of Contract award, provide a security for the due performance of the Contract in the amount in Indian Rupees (INR)**.**
ii. The security shall be a bank guarantee in the form provided in the Sample Contractual Forms Section of the bidding documents, or it shall be in another form acceptable to BMC.
iii. The security shall automatically become null and void once all the obligations of the Managed / Cloud Service Provider under the Contract have been fulfilled, including, but not limited to, any obligations during the Warranty Period and any extensions to the period. The security shall be returned to the Managed / Cloud Service Provider no later than ninety (90) days after its expiration.
iv. Upon Operational Acceptance of the entire System, the security shall be reduced to the amount **specified in the BDS,** on the date of such Operational Acceptance, so that the reduced security would only cover the remaining warranty obligations of the Cloud Service Provider.

14. Taxes and Duties

a. For Goods or Services supplied from outside India, the Managed / Cloud Service Provider shall be entirely responsible for all taxes excluding GST, stamp duties, license fees, and other such levies imposed outside India.

b. For Goods or Services supplied locally, the Managed / Cloud Service Provider shall be entirely responsible for all taxes, duties, license fees, etc., incurred until delivery of the contracted Goods or Services to BMC.

c. If any tax exemptions, reductions, allowances, or privileges may be available to the Managed / Cloud Service Provider in India, BMC shall use its best efforts to enable the Managed / Cloud Service Provider to benefit from any such tax savings to the maximum allowable extent.

d. For the purpose of the Contract, it is agreed that the Contract Price specified in Article 2 (Contract Price and Terms of Payment) of the Contract Agreement is based on the taxes, duties, levies, and charges prevailing at the date thirty (30) days prior to the date of bid submission in India (also called "Tax" in this GCC Clause (Taxes and Duties). 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 Cloud Service Provider, its Subcontractors, 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.

D. INTELLECTUAL PROPERTY

15. Copyright

a. The Intellectual Property Rights in all Standard Software and Standard Materials shall remain vested in the owner of such rights.

b. BMC agrees to restrict use, copying, or duplication of the Standard Software and Standard Materials in accordance with GCC Clause (Software License Agreements), except that additional copies of Standard Materials may be made by BMC for use within the scope of the project of which the System is a part, in the event that the Managed / Cloud Service Provider does not deliver copies within thirty (30) days from receipt of a request for such Standard Materials.

c. BMC's contractual rights to use the Standard Software or elements of the Standard Software may not be assigned, licensed, or otherwise transferred voluntarily except in accordance with the relevant license agreement to a legally constituted successor organization (e.g., a reorganization of a public entity formally authorized by the government or through a merger or acquisition of a private entity).

d. The Intellectual Property Rights in all Custom Software and Custom Materials specified in Appendices 4 and 5 of 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 BMC. The Managed / Cloud Service Provider shall do and execute or arrange for the doing and executing of each necessary act, document, and thing that BMC may consider necessary or desirable to perfect the right, title, and interest of BMC in and to those rights. In respect of such Custom Software and Custom Materials, the Managed / Cloud Service Provider shall ensure that the holder of a moral right in such an item does not assert it, and the Managed / Cloud Service Provider shall, if requested to do so by BMC and where permitted by applicable law, ensure that the holder of such a moral right waives it.

16. Software License Agreements

a. Except to the extent that the Intellectual Property Rights in the Software vest in BMC, the Managed / Cloud Service Provider hereby grants to BMC license to access and use the Software, including all inventions, designs, and marks embodied in the Software.

Such license to access and use the Software shall:

a. be:

i. nonexclusive;

ii. fully paid up and irrevocable (except that it shall terminate if the Contract terminates under relevant GCC Clauses (Termination);

iii. valid throughout the territory of India;

iv. subject to NO additional restrictions.

b. permit the Software to be:

i. used or copied for use on or with the computer(s) for which it was acquired (if specified in the Technical Requirements and/or the Cloud Service Provider'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;

ii. used or copied for use on or transferred to a replacement computer(s), (and use on the original and replacement computer(s) may be simultaneous during a reasonable transitional period) provided that, if the Technical Requirements and/or the Cloud Service Provider's bid specifies a class of computer to which the

license is restricted, the replacement computer(s) is(are) within that class;

c. 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;

d. reproduced for safekeeping or backup purposes;

e. customized, adapted, or combined with other computer software for use by BMC, 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;

f. disclosed to, and reproduced for use by, support service Cloud Service Providers and their subcontractors, (and BMC may sublicense such persons to use and copy for use the Software) to the extent reasonably necessary to the performance of their support service contracts, subject to the same restrictions as are set forth in this Contract; and

g. disclosed to, and reproduced for use by, NO other parties.

b. The Managed / Cloud Service Provider has the right to audit the Standard Software to verify compliance with the above license agreements. BMC will make available to the Cloud Service Provider, within seven (7) days of a written request, accurate and up-to-date records of the number and location of copies, the number of authorized users, or any other relevant data required to demonstrate use of the Standard Software as per the license agreement. If and only if, expressly agreed in writing between BMC and the Cloud Service Provider, BMC will allow, under a pre-specified agreed procedure, the execution of embedded software functions under Cloud Service Provider's control, and unencumbered transmission of resulting information on software usage.

17. Confidential Information

a. The "Receiving Party" (either BMC or the Cloud Service Provider) 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.

b. For the purposes of GCC Clause (Confidential Information), the Managed / Cloud Service Provider is also deemed to be the Receiving Party of Confidential Information generated by the Managed / Cloud Service Provider itself in the course of the performance of its obligations under the Contract and relating to the businesses, finances, Cloud Service Providers, employees, or other contacts of BMC or BMC's use of the System.

c. Notwithstanding relevant GCC Clauses (Confidential Information):

i. the Managed / Cloud Service Provider may furnish to its Subcontractor Confidential Information of BMC to the extent reasonably required for the Subcontractor to perform its work under the Contract; and

ii. BMC may furnish Confidential Information of the Cloud Service Provider: (i) to its other support Service Providers and their subcontractors 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 (Confidential Information) as if that person were party to the Contract in place of the Receiving Party.

d. BMC shall not, without the Cloud Service Provider's prior written consent, use any Confidential Information received from the Managed / Cloud Service Provider for any purpose other than the operation, and maintenance. Similarly, the Managed / Cloud Service Provider shall not, without BMC's prior written consent, use any Confidential Information received from BMC for any purpose other than those that are required for the performance of the Contract.

e. The obligation of a party under relevant GCC Clauses (Confidential Information) above, however, shall not apply to that information which:
   i. now or hereafter enters the public domain through no fault of the Receiving Party;
   ii. 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;
   iii. otherwise lawfully becomes available to the Receiving Party from a third party that has no obligation of confidentiality.

f. The above provisions of this GCC Clause (Confidential Information) 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.

g. The provisions of this GCC Clause (Confidential Information) shall survive the termination, for whatever reason, of the Contract for three (3) years.

E. Supply, Installation, Testing, Commissioning, and Acceptance of the System

18. Representatives

a. Project Manager

If the Project Manager is not named in the Contract, then within fourteen (14) days of the Effective Date, BMC shall appoint and notify the Managed / Cloud Service Provider in writing of the name of the Project Manager. BMC may from time to time appoint some other person as the Project Manager in place of the person previously so appointed and shall give notice of the name of such other person to the Managed / Cloud Service Provider 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 Cloud Service Provider. The Project Manager shall have the authority to represent BMC 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 BMC pursuant to GCC Clause (Notices).

b. Cloud Service Provider's Representative

   i. If the Cloud Service Provider's Representative is not named in the Contract, then within fourteen (14) days of the Effective Date, the Managed / Cloud Service Provider shall appoint the Cloud Service Provider's Representative and shall request BMC 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 Cloud Service Provider's Representative. If BMC does not object to the appointment within fourteen (14) days, the Cloud Service Provider's Representative shall be deemed to have been approved. If BMC objects to the appointment within fourteen (14) days giving the reason therefor, then the Managed / Cloud Service Provider shall appoint a replacement within fourteen (14) days of such objection in accordance with this GCC Clause (Representatives).

   ii. The Cloud Service Provider's Representative shall have the authority to represent the Managed / Cloud Service Provider 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 Managed / Cloud Service Provider pursuant to GCC Clause (Notices).

iii. The Managed / Cloud Service Provider shall not revoke the appointment of the Cloud Service Provider's Representative without BMC's prior written consent, which shall not be unreasonably withheld. If BMC consents to such an action, the Managed / Cloud Service Provider shall appoint another person of equal or superior qualifications as the Cloud Service Provider's Representative, pursuant to the procedure set out in GCC Clause (Representatives).

iv. The Cloud Service Provider's Representative and staff are obliged to work closely with BMC's Project Manager and staff, act within their own authority, and abide by directives issued by BMC that are consistent with the terms of the Contract. The Cloud Service Provider's Representative is responsible for managing the activities of its personnel and any subcontracted personnel.

v. The Cloud Service Provider's Representative may, subject to the approval of BMC (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 Cloud Service Provider'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.

vi. Any act or exercise by any person of powers, functions and authorities so delegated to him or her in accordance with GCC Clause (Representatives) shall be deemed to be an act or exercise by the Cloud Service Provider's Representative.

c. Objections and Removals

i. BMC may by notice to the Managed / Cloud Service Provider object to any representative or person employed by the Managed / Cloud Service Provider in the execution of the Contract who, in the reasonable opinion of BMC, may have behaved inappropriately, be incompetent, or be negligent. BMC shall provide evidence of the same, whereupon the Managed / Cloud Service Provider shall remove such person from work on the System.

ii. If any representative or person employed by the Managed / Cloud Service Provider is removed in accordance with GCC Clause (Representatives), the Managed / Cloud Service Provider shall, where required, promptly appoint a replacement.

19. Project Plan

a. In close cooperation with BMC and based on the Preliminary Project Plan included in the Cloud Service Provider's bid, the Managed / Cloud Service Provider shall develop a Project Plan encompassing the activities specified in the Contract. The contents of the Project Plan shall be as specified in the Section – BMC's Requirements.

b. Within *thirty (30)* days from the Effective Date of the Contract, the Managed / Cloud Service Provider shall present a Project Plan to BMC. BMC shall, within *fourteen (14)* days of receipt of the Project Plan, notify the Managed / Cloud Service Provider 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 Information Technologies will satisfy the Technical Requirements (in this Clause, called "non-conformities" below). The Managed / Cloud Service Provider shall, within *five (5)* days of receipt of such notification, correct the Project Plan and resubmit to BMC. BMC shall, within *five (5)* days of resubmission of the Project Plan, notify the Managed / Cloud Service Provider 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, BMC shall provide confirmation in writing to the Cloud Service Provider. This approved Project Plan

("the Agreed Project Plan") shall be contractually binding on BMC and the Cloud Service Provider.

c. If required, the impact on the Implementation Schedule of modifications agreed during finalization of the Agreed Project Plan shall be incorporated in the Contract by amendment, in accordance with relevant GCC Clauses (Changes to the System) and (Extension of Time for Achieving Operational Acceptance).

d. The Managed / Cloud Service Provider shall undertake to supply, install, test, and commission the System in accordance with the Agreed Project Plan and the Contract.

e. The Managed / Cloud Service Provider shall submit to BMC Monthly Progress Reports summarizing:

   i. results accomplished during the prior period;

   ii. cumulative deviations to date from schedule of progress milestones as specified in the Agreed Project Plan;

   iii. corrective actions to be taken to return to planned schedule of progress; proposed revisions to planned schedule;

   iv. other issues and outstanding problems; proposed actions to be taken;

   v. resources that the Managed / Cloud Service Provider expects to be provided by BMC and/or actions to be taken by BMC in the next reporting period;

   vi. other issues or potential problems the Managed / Cloud Service Provider foresees that could impact on project progress and/or effectiveness.

f. The Managed / Cloud Service Provider shall submit to BMC other (periodic) reports as specified in the Section – BMC's Requirements.

20. Subcontracting

a. Appendix 3 (List of Approved Subcontractors) to the Contract Agreement specifies critical items of supply or services and a list of Subcontractors for each item that are considered acceptable by BMC. If no Subcontractors are listed for an item, the Managed / Cloud Service Provider shall prepare a list of Subcontractors it considers qualified and wishes to be added to the list for such items. The Managed / Cloud Service Provider may from time to time propose additions to or deletions from any such list. The Managed / Cloud Service Provider shall submit any such list or any modification to the list to BMC for its approval in sufficient time so as not to impede the progress of work on the System. BMC shall not withhold such approval unreasonably. Such approval by BMC of a Subcontractor(s) shall not relieve the Managed / Cloud Service Provider from any of its obligations, duties, or responsibilities under the Contract.

b. The Managed / Cloud Service Provider may, at its discretion, select and employ Subcontractors for such critical items from those Subcontractors listed pursuant to GCC Clause (Subcontracting). If the Managed / Cloud Service Provider wishes to employ a Subcontractor not so listed, or subcontract an item not so listed, it must seek BMC's prior approval under GCC Clause (Subcontracting).

c. For items for which pre-approved Subcontractor lists have not been specified in Appendix 3 to the Contract Agreement, the Managed / Cloud Service Provider may employ such Subcontractors as it may select, provided: (i) the Managed / Cloud Service Provider notifies BMC in writing at least thirty (30) days prior to the proposed mobilization date for such Subcontractor; and (ii) by the end of this period either BMC has granted its approval in writing or fails to respond. The Managed / Cloud Service Provider shall not engage any Subcontractor to which BMC has objected in writing prior to the end of the notice period. The absence of a written objection by BMC during the above specified period shall constitute formal acceptance of the proposed Subcontractor. Except to the extent that it permits the deemed approval of BMC of Subcontractors not listed in the Contract Agreement, nothing in this Clause, however,

shall limit the rights and obligations of either BMC or Managed / Cloud Service Provider as they are specified in relevant GCC Clauses (Subcontracting), or in Appendix 3 of the Contract Agreement.

21. Design and Engineering

a. Technical Specifications and Drawings

i. The Managed / Cloud Service Provider shall execute the basic and detailed design and the implementation activities necessary for successful installation of the System in compliance with the provisions of the Contract or, where not so specified, in accordance with good industry practice.

The Managed / Cloud Service Provider shall be responsible for any discrepancies, errors or omissions in the specifications, drawings, and other technical documents that it has prepared, whether such specifications, drawings, and other documents have been approved by the Project Manager or not, provided that such discrepancies, errors, or omissions are not because of inaccurate information furnished in writing to the Managed / Cloud Service Provider by or on behalf of BMC.

ii. The Managed / Cloud Service Provider shall be entitled to disclaim responsibility for any design, data, drawing, specification, or other document, or any modification of such design, drawings, specification, or other documents provided or designated by or on behalf of BMC, by giving a notice of such disclaimer to the Project Manager.

b. Codes and Standard

i. Wherever references are made in the Contract to codes and standards in accordance with which the Contract shall be executed, the edition or the revised version of such codes and standards current at the date thirty (30) days prior to date of bid submission shall apply. During Contract execution, any changes in such codes and standards shall be applied after approval by BMC and shall be treated in accordance with GCC Clause (Changes to the System).

c. Approval/Review of Controlling Technical Documents by the Project Manager

i. There will NO Controlling Technical Documents required. However, if the Section – BMC's Requirements specifies Controlling Technical Documents, the Managed / Cloud Service Provider shall prepare and furnish such documents for the Project Manager's approval or review.

Any part of the System covered by or related to the documents to be approved by the Project Manager shall be executed only after the Project Manager's approval of these documents.

Relevant GCC Clauses (Design and Engineering) shall apply to those documents requiring the Project Manager's approval, but not to those furnished to the Project Manager for its review only.

ii. Within fourteen (14) days after receipt by the Project Manager of any document requiring the Project Manager's approval in accordance with GCC Clause ((Design and Engineering), the Project Manager shall either return one copy of the document to the Managed / Cloud Service Provider with its approval endorsed on the document or shall notify the Managed / Cloud Service Provider in writing of its disapproval of the document and the reasons for disapproval and the modifications that the Project Manager proposes. If the Project Manager fails to take such action within the fourteen (14) days, then the document shall be deemed to have been approved by the Project Manager.

iii. The Project Manager shall not disapprove any document except on the grounds that the document does not comply with some specified provision of the Contract or that it is contrary to good industry practice.

iv. If the Project Manager disapproves the document, the Managed / Cloud Service Provider shall modify the document and resubmit it for the Project Manager's approval in accordance with GCC Clause (Design and Engineering). If the Project Manager approves the document subject to modification(s), the Managed / Cloud Service Provider shall make the required modification(s), and the document shall then be deemed to have been approved, subject to GCC Clause (Design and Engineering). The procedure set out in relevant GCC Clauses (Design and Engineering) shall be repeated, as appropriate, until the Project Manager approves such documents.

v. If any dispute occurs between BMC and the Managed / Cloud Service Provider in connection with or arising out of the disapproval by the Project Manager of any document and/or any modification(s) to a document that cannot be settled between the parties within a reasonable period, then, in case the Contract Agreement includes and names an Adjudicator, such dispute may be referred to the Adjudicator for determination in accordance with GCC Clause (Adjudicator). If such dispute is referred to an Adjudicator, the Project Manager shall give instructions as to whether and if so, how, performance of the Contract is to proceed. The Managed / Cloud Service Provider shall proceed with the Contract in accordance with the Project Manager's instructions, provided that if the Adjudicator upholds the Cloud Service Provider's view on the dispute and if BMC has not given notice under GCC Clause (Adjudication), then the Managed / Cloud Service Provider shall be reimbursed by BMC for any additional costs incurred by reason of such instructions and shall be relieved of such responsibility or liability in connection with the dispute and the execution of the instructions as the Adjudicator shall decide, and the Time for Achieving Operational Acceptance shall be extended accordingly.

vi. The Project Manager's approval, with or without modification of the document furnished by the Cloud Service Provider, shall not relieve the Managed / Cloud Service Provider of any responsibility or liability imposed upon it by any provisions of the Contract except to the extent that any subsequent failure results from modifications required by the Project Manager or inaccurate information furnished in writing to the Managed / Cloud Service Provider by or on behalf of BMC.

vii. The Managed / Cloud Service Provider shall not depart from any approved document unless the Managed / Cloud Service Provider has first submitted to the Project Manager an amended document and obtained the Project Manager's approval of the document, pursuant to the provisions of this GCC Clause (Design and Engineering). If the Project Manager requests any change in any already approved document and/or in any document based on such an approved document, the provisions of GCC Clause (Changes to the System) shall apply to such request.

22. Procurement, Delivery, and Transport

a. Subject to related BMC's responsibilities pursuant to relevant GCC Clauses (BMC's Responsibilities) and (Taxes and Duties), the Managed / Cloud Service Provider shall manufacture or procure and transport all the Information Technologies, Materials, and other Goods in an expeditious and orderly manner to the Project Site.

b. Delivery of the Information Technologies, Materials, and other Goods shall be made by the Managed / Cloud Service Provider in accordance with the Technical Requirements.

c. Early or partial deliveries require the explicit written consent of BMC, which consent shall not be unreasonably withheld.

d. Transportation

   i. The Managed / Cloud Service Provider shall provide such packing of the Goods as is required to prevent their damage or deterioration during shipment. The packing, marking, and documentation within and outside the packages shall comply strictly with BMC's instructions to the Cloud Service Provider.

   ii. The Managed / Cloud Service Provider will bear responsibility for and cost of transport to the Project Sites in accordance with the terms and conditions used in the specification of prices in the Price Schedules, including the terms and conditions of the associated Incoterms.

   iii. The Managed / Cloud Service Provider shall be free to use transportation through carriers registered in any eligible country and to obtain insurance from any eligible source country.

e. The Managed / Cloud Service Provider will provide BMC with shipping and other documents, as specified below:

   i. For Goods supplied from outside India:

      Upon shipment, the Managed / Cloud Service Provider shall notify BMC and the insurance company contracted by the Managed / Cloud Service Provider to provide cargo insurance by telex, cable, facsimile, electronic mail, or EDI with the full details of the shipment. The Managed / Cloud Service Provider shall promptly send the following documents to BMC by mail or courier, as appropriate, with a copy to the cargo insurance company:

      1. two copies of the Cloud Service Provider's invoice showing the description of the Goods, quantity, unit price, and total amount;
      2. usual transportation documents;
      3. insurance certificate;
      4. certificate(s) of origin; and
      5. estimated time and point of arrival in India and at the site.

   ii. For Goods supplied locally (i.e., from within India):

      Upon shipment, the Managed / Cloud Service Provider shall notify BMC by telex, cable, facsimile, electronic mail, or EDI with the full details of the shipment. The Managed / Cloud Service Provider shall promptly send the following documents to BMC by mail or courier, as appropriate:

      1. two copies of the Cloud Service Provider's invoice showing the Goods' description, quantity, unit price, and total amount;
      2. delivery note, railway receipt, or truck receipt;
      3. certificate of insurance;
      4. certificate(s) of origin; and
      5. estimated time of arrival at the site.

f. Customs Clearance

   i. The Managed / Cloud Service Provider will bear responsibility for, and cost of, customs clearance into India in accordance the particular Incoterm(s) used for Goods supplied from outside India in the Price Schedules referred to by Article 2 of the Contract Agreement.

ii. In the event of delays in customs clearance that are not the fault of the Cloud Service Provider, the Managed / Cloud Service Provider shall be entitled to an extension in the Time for Achieving Operational Acceptance, pursuant to GCC Clause (Extension of Time for Achieving Operational Acceptance);

23. Product Upgrades

a. At any point during performance of the Contract, should technological advances be introduced by the Original Equipment Manufacturer (OEM) or by the Managed / Cloud Service Provider for Information Technologies originally offered by the Managed / Cloud Service Provider in its bid and still to be delivered, the Managed / Cloud Service Provider shall be obligated to offer to BMC the latest versions of the available Information Technologies having equal or better performance or functionality at the same or lesser unit prices, pursuant to GCC Clause (Changes to the System).

b. At any point during performance of the Contract, for Information Technologies still to be delivered, the Managed / Cloud Service Provider will also pass on to BMC any cost reductions and additional and/or improved support and facilities that it offers to other clients of the Managed / Cloud Service Provider in India, pursuant to GCC Clause (Changes to the System).

c. During performance of the Contract, the Managed / Cloud Service Provider shall offer to BMC 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 Original Equipment Manufacturer (OEM) or by the Managed / Cloud Service Provider to other clients of the Managed / Cloud Service Provider in India, and no later than three (3) months after they are released in the country of origin. In no case will the prices for these Software exceed those quoted by the Managed / Cloud Service Provider in the Recurrent Costs tables in its bid.

d. During the Warranty Period, the Managed / Cloud Service Provider will provide at no additional cost to BMC all new versions, releases, and updates for all Standard Software that are used in the System, within thirty (30) days of their availability from the Original Equipment Manufacturer (OEM) or by the Managed / Cloud Service Provider to other clients of the Managed / Cloud Service Provider in India, and no later than three(3) months after they are released in the country of origin of the Software.

e. BMC shall introduce all new versions, releases or updates of the Software within three (3) 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 Managed / Cloud Service Provider 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 Managed / Cloud Service Provider stop supporting or maintaining a version or release of the Software less than twenty-four (24) months after BMC receives a production-ready copy of a subsequent version, release, or update. BMC 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.

24. **Implementation, Installation, and Other Services**

a. The Managed / Cloud Service Provider shall provide all Services specified in the Contract and Agreed Project Plan in accordance with the highest standards of professional competence and integrity.

b. Prices charged by the Managed / Cloud Service Provider 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 Managed / Cloud Service Provider in the Recurrent Cost Schedules of its Bid) and shall not exceed the prevailing rates

charged by the Managed / Cloud Service Provider to other purchasers in India for similar services.

25. **Inspections and Tests**

a. BMC or its representative shall have the right to inspect and/or test any components of the System, as specified in the Technical Requirements, to confirm their good working order and/or conformity to the Contract at the point of delivery and/or at the Project Site.

b. BMC or its representative shall be entitled to attend any such inspections and/or tests of the components, provided that BMC 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.

c. Should the inspected or tested components fail to conform to the Contract, BMC may reject the component(s), and the Managed / Cloud Service Provider shall either replace the rejected component(s), or make alterations as necessary so that it meets the Contract requirements free of cost to BMC.

d. The Project Manager may require the Managed / Cloud Service Provider to carry out any inspection and/or test not specified in the Contract, provided that the Cloud Service Provider'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 impedes the progress of work on the System and/or the Cloud Service Provider'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.

e. 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 (Settlement of Disputes), starting with referral of the matter to the Adjudicator in case an Adjudicator is included and named in the Contract Agreement.

26. **Installation of the System**

a. As soon as the System, or any Subsystem, has, in the opinion of the Cloud Service Provider, been delivered, pre-commissioned, and made ready for Commissioning and Operational Acceptance Testing in accordance with the Technical Requirements, the Agreed Project Plan, the Managed / Cloud Service Provider shall so notify BMC in writing.

b. The Project Manager shall, within fourteen (14) days after receipt of the Cloud Service Provider's notice under GCC Clause (Installation of the System), either issue an Installation Certificate in the form specified in the Sample Contractual Forms Section in the bidding documents, stating that the System, or major component or Subsystem (if Acceptance by major component or Subsystem is specified pursuant to the GCC Clause (Commissioning and Operational Acceptance), has achieved Installation by the date of the Cloud Service Provider's notice under GCC Clause (Installation of the System), or notify the Managed / Cloud Service Provider 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 Managed / Cloud Service Provider shall use all reasonable endeavors to promptly remedy any defect and/or deficiencies that the Project Manager has notified the Managed / Cloud Service Provider of. The Managed / Cloud Service Provider shall then promptly carry out retesting of the System or Subsystem and, when in the Cloud Service Provider's opinion the System or Subsystem is ready for Commissioning and Operational Acceptance Testing, notify BMC in writing, in accordance with GCC Clause (Installation of the System). The procedure set out in this GCC Clause (Installation of the System) shall be repeated, as necessary, until an Installation Certificate is issued.

c. If the Project Manager fails to issue the Installation Certificate and fails to inform the Managed / Cloud Service Provider of any defects and/or deficiencies within fourteen (14) days after receipt of the Cloud Service Provider's notice under GCC Clause (Installation of the System), or if BMC 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 Cloud Service Provider's notice or repeated notice, or when BMC put the System into production operation, as the case may be.

27. **Commissioning and Operational Acceptance**

a. Commissioning

i. Commissioning of the System (or Subsystem if specified pursuant to the GCC Clause (Commissioning and Operational Acceptance) shall be commenced by the Cloud Service Provider:

1. immediately after the Installation Certificate is issued by the Project Manager, pursuant to GCC Clause (Installation of the System); or
2. as otherwise specified in the Technical Requirement or the Agreed Project Plan; or
3. immediately after Installation is deemed to have occurred, under GCC Clause (Installation of the System).

ii. BMC shall supply the operating and technical personnel and all materials and information reasonably required to enable the Managed / Cloud Service Provider 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.

b. Operational Acceptance Tests

i. The Operational Acceptance Tests (and repeats of such tests) shall be the primary responsibility of BMC (in accordance with GCC Clause (BMC's Responsibilities)), but shall be conducted with the full cooperation of the Managed / Cloud Service Provider during Commissioning of the System (or major components or Subsystem[s]), to ascertain whether the System (or major component or Subsystem[s]) conforms to the Technical Requirements and meets the standard of performance quoted in the Cloud Service Provider's bid, including, but not restricted to, the functional and technical performance requirements. The Operational Acceptance Tests during Commissioning will be conducted as specified in the Technical Requirements and/or the Agreed Project Plan.
At BMC's discretion, Operational Acceptance Tests may also be performed on replacement Goods, upgrades and new version releases, and Goods that are added or field-modified after Operational Acceptance of the System.

ii. If for reasons attributable to BMC, the Operational Acceptance Test of the System (or Subsystem[s] or major components, pursuant to the GCC Clause (Commissioning and Operational Acceptance)) cannot be successfully completed within ninety (90) days from the date of Installation or any other period agreed upon in writing by BMC and the Cloud Service Provider, the Managed / Cloud Service Provider shall be deemed to have fulfilled its obligations with respect to the technical and functional aspects of the Technical Specifications, and/or the Agreed Project Plan, and relevant GCC Clauses (Operational Acceptance Time Guarantee) shall not apply.

c. Operational Acceptance

i. Subject to GCC Clause (Commissioning and Operational Acceptance – Sub-Clause Partial Acceptance) below, Operational Acceptance shall occur in respect of the System, when

1. the Operational Acceptance Tests, as specified in the Technical Requirements, and/or the Agreed Project Plan have been successfully completed; or
2. the Operational Acceptance Tests have not been successfully completed or have not been carried out for reasons that are attributable to BMC within the period from the date of Installation or any other agreed-upon period as specified in GCC Clause (Commissioning and Operational Acceptance) above; or
3. BMC 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 Managed / Cloud Service Provider shall notify BMC and document such use.

ii. At any time after any of the events set out in GCC Clause (Commissioning and Operational Acceptance) have occurred, the Managed / Cloud Service Provider may give a notice to the Project Manager requesting the issue of an Operational Acceptance Certificate.

iii. After consultation with BMC, and within fourteen (14) days after receipt of the Cloud Service Provider's notice, the Project Manager shall:
   1. issue an Operational Acceptance Certificate; or
   2. notify the Managed / Cloud Service Provider in writing of any defect or deficiencies or other reason for the failure of the Operational Acceptance Tests; or
   3. issue the Operational Acceptance Certificate, if the situation covered by GCC Clause (Commissioning and Operational Acceptance) arises.

iv. The Managed / Cloud Service Provider shall use all reasonable endeavors 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 Managed / Cloud Service Provider of. Once such remedies have been made by the Cloud Service Provider, the Managed / Cloud Service Provider shall notify BMC, and BMC, with the full cooperation of the Cloud Service Provider, shall use all reasonable endeavors to promptly carry out retesting of the System or Subsystem. Upon the successful conclusion of the Operational Acceptance Tests, the Managed / Cloud Service Provider shall notify BMC of its request for Operational Acceptance Certification, in accordance with GCC Clause (Commissioning and Operational Acceptance). BMC shall then issue to the Managed / Cloud Service Provider the Operational Acceptance Certification in accordance with GCC Clause (Commissioning and Operational Acceptance), or shall notify the Managed / Cloud Service Provider of further defects, deficiencies, or other reasons for the failure of the Operational Acceptance Test. The procedure set out in this GCC Clause (Commissioning and Operational Acceptance) shall be repeated, as necessary, until an Operational Acceptance Certificate is issued.

v. If the System or Subsystem fails to pass the Operational Acceptance Test(s) in accordance with GCC Clause (Commissioning and Operational Acceptance), then either:
   1. BMC may consider terminating the Contract, pursuant to GCC Clause (Termination); or
   2. if the failure to achieve Operational Acceptance within the specified time period is a result of the failure of BMC to fulfill its obligations under the Contract, then the Managed / Cloud Service Provider shall be deemed to have fulfilled its obligations with respect to the relevant technical and functional aspects of the Contract, and relevant GCC Clauses (Functional Guarantees) shall not apply.

vi. If within fourteen (14) days after receipt of the Cloud Service Provider's notice the Project Manager fails to issue the Operational Acceptance Certificate or fails to inform the Managed / Cloud Service Provider 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 Cloud Service Provider's said notice.

d. Partial Acceptance
   i. If so specified in this GCC Clause (Commissioning and Operational Acceptance), Installation and Commissioning shall be carried out individually for each identified major component or Subsystem(s) of the System. In this event, the provisions in the Contract relating to Installation and Commissioning, including the Operational Acceptance Test, shall apply to each such major component or Subsystem individually, and Operational Acceptance Certificate(s) shall be issued accordingly for each such major component or Subsystem of the System, subject to the limitations contained in GCC Clause (Commissioning and Operational Acceptance).
   ii. The issuance of Operational Acceptance Certificates for individual major components or Subsystems pursuant to GCC Clause (Commissioning and Operational Acceptance) shall not relieve the Managed / Cloud Service Provider of its obligation to obtain an Operational Acceptance Certificate for the System as an integrated whole (if so specified in the GCC Clauses (Terms of Payment) and (Commissioning and Operational Acceptance)) once all major components and Subsystems have been supplied, installed, tested, and commissioned.
   iii. In the case of minor components for the System that by their nature do not require Commissioning or an Operational Acceptance Test (e.g., minor fittings, furnishings or site works, etc.), the Project Manager shall issue an Operational Acceptance Certificate within fourteen (14) days after the fittings and/or furnishings have been delivered and/or installed or the site works have been completed. The Managed / Cloud Service Provider shall, however, use all reasonable endeavors to promptly remedy any defects or deficiencies in such minor components detected by BMC or Cloud Service Provider.

F. GUARANTEES AND LIABILITIES

28. Operational Acceptance Time Guarantee

a. The Managed / Cloud Service Provider guarantees that it shall complete the supply, Installation, Commissioning, and achieve Operational Acceptance of the System (or Subsystems, pursuant to the GCC Clause (Commissioning and Operational Acceptance) within the time periods specified in the Implementation Schedule and/or the Agreed Project Plan pursuant to GCC Clause (Time for Commencement and Acceptance), or within such extended time to which the Managed / Cloud Service Provider shall be entitled under GCC Clause (Extension of Time for Achieving Operational Acceptance).

b. If the Managed / Cloud Service Provider fails to supply, install, commission, and achieve Operational Acceptance of the System (or Subsystems pursuant to the GCC Clause (Commissioning and Operational Acceptance) within the time for achieving Operational Acceptance specified in the Implementation Schedule or the Agreed Project Plan, or any extension of the time for achieving Operational Acceptance previously granted under GCC Clause (Extension of Time for Achieving Operational Acceptance), the Managed / Cloud Service Provider shall pay to BMC liquidated damages at the rate of one half of one percent per week as a percentage of the Contract Price (exclusive of Recurrent Costs if any), 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 of ten (10) percent of the Contract Price (exclusive of Recurrent Costs if any). Once the Maximum is reached, BMC may consider termination of the Contract, pursuant to GCC Clause (Termination).

c. Liquidated damages payable under GCC Clause (Operational Acceptance Time Guarantee) shall apply only to the failure to achieve Operational Acceptance of the System (and Subsystems) as specified in the Implementation Schedule and/or Agreed Project Plan. This Clause (Operational Acceptance Time Guarantee) shall

not limit, however, any other rights or remedies BMC may have under the Contract for other delays.

d. If liquidated damages are claimed by BMC for the System (or Subsystem), the Managed / Cloud Service Provider shall have no further liability whatsoever to BMC 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 Managed / Cloud Service Provider from any of its obligations to complete the System or from any other of its obligations and liabilities under the Contract.

29. Defect Liability

a. The Managed / Cloud Service Provider warrants that the System, including all Information Technologies, Materials, and other Goods supplied and Services provided, shall be free from defects in the design, engineering, Materials, and workmanship that prevent the System and/or any of its components from fulfilling the Technical Requirements or that limit in a material fashion the performance, reliability, or extensibility of the System and/or Subsystems. There will be NO exceptions and/or limitations to this warranty with respect to Software (or categories of Software). Commercial warranty provisions of products supplied under the Contract shall apply to the extent that they do not conflict with the provisions of this Contract.

b. The Managed / Cloud Service Provider also warrants that the Information Technologies, Materials, and other Goods supplied under the Contract are new, unused, and incorporate all recent improvements in design that materially affect the System's or Subsystem's ability to fulfill the Technical Requirements.

c. The Managed / Cloud Service Provider warrants that: (i) all Goods components to be incorporated into the System form part of the Cloud Service Provider's and/or Subcontractor's current product lines, and (ii) they have been previously released to the market.

d. The Warranty Period shall commence from the date of Operational Acceptance of the System (or of any major component or Subsystem for which separate Operational Acceptance is provided for in the Contract).

e. If during the Warranty Period any defect as described in GCC Clause (Defect Liability) should be found in the design, engineering, Materials, and workmanship of the Information Technologies and other Goods supplied or of the Services provided by the Cloud Service Provider, the Managed / Cloud Service Provider shall promptly, in consultation and agreement with BMC regarding appropriate remedying of the defects, and at its sole cost, repair, replace, or otherwise make good (as the Managed / Cloud Service Provider shall, at its discretion, determine) such defect as well as any damage to the System caused by such defect. Any defective Information Technologies or other Goods that have been replaced by the Managed / Cloud Service Provider shall remain the property of the Cloud Service Provider.

f. The Managed / Cloud Service Provider shall not be responsible for the repair, replacement, or making good of any defect, or of any damage to the System arising out of or resulting from any of the following causes:

   i. improper operation or maintenance of the System by BMC;

   ii. normal wear and tear;

   iii. use of the System with items not supplied by the Cloud Service Provider, unless otherwise identified in the Technical Requirements, or approved by the Cloud Service Provider; or

   iv. modifications made to the System by BMC, or a third party, not approved by the Cloud Service Provider.

g. The Cloud Service Provider's obligations under this GCC Clause (Defect Liability) shall not apply to:

i. any materials that are normally consumed in operation or have a normal life shorter than the Warranty Period; or

ii. any designs, specifications, or other data designed, supplied, or specified by or on behalf of BMC or any matters for which the Managed / Cloud Service Provider has disclaimed responsibility, in accordance with GCC Clause (Design and Engineering).

h. BMC shall give the Managed / Cloud Service Provider a notice promptly following the discovery of such defect, stating the nature of any such defect together with all available evidence. BMC shall afford all reasonable opportunity for the Managed / Cloud Service Provider to inspect any such defect. BMC shall afford the Managed / Cloud Service Provider all necessary access to the System and the site to enable the Managed / Cloud Service Provider to perform its obligations under this GCC Clause (Defect Liability).

i. The Managed / Cloud Service Provider may, with the consent of BMC, remove from the site any Information Technologies and other Goods that are defective, if the nature of the defect, and/or any damage to the System caused by the defect, is such that repairs cannot be expeditiously carried out at the site. If the repair, replacement, or making good is of such a character that it may affect the efficiency of the System, BMC may give the Managed / Cloud Service Provider notice requiring that tests of the defective part be made by the Managed / Cloud Service Provider immediately upon completion of such remedial work, whereupon the Managed / Cloud Service Provider shall carry out such tests.

   If such part fails the tests, the Managed / Cloud Service Provider shall carry out further repair, replacement, or making good (as the case may be) until that part of the System passes such tests. The tests shall be agreed upon by BMC and the Cloud Service Provider.

j. The response times and repair/replacement times for Warranty Defect Repair are specified in the Technical Requirements. Nevertheless, if the Managed / Cloud Service Provider fails to commence the work necessary to remedy such defect or any damage to the System caused by such defect within two weeks BMC may, following notice to the Cloud Service Provider, proceed to do such work or contract a third party (or parties) to do such work, and the reasonable costs incurred by BMC in connection with such work shall be paid to BMC by the Managed / Cloud Service Provider or may be deducted by BMC from any monies due the Managed / Cloud Service Provider or claimed under the Performance Security.

k. If the System or Subsystem cannot be used by reason of such defect and/or making good of such defect, the Warranty Period for the System shall be extended by a period equal to the period during which the System or Subsystem could not be used by BMC because of such defect and/or making good of such defect.

l. Items substituted for defective parts of the System during the Warranty Period shall be covered by the Defect Liability Warranty for the remainder of the Warranty Period applicable for the part replaced or three (3) months, whichever is greater. For reasons of information security, BMC may choose to retain physical possession of any replaced defective information storage devices.

m. At the request of BMC and without prejudice to any other rights and remedies that BMC may have against the Managed / Cloud Service Provider under the Contract, the Managed / Cloud Service Provider will offer all possible assistance to BMC to seek warranty services or remedial action from any subcontracted third-party producers or licensor of Goods included in the System, including without limitation assignment or transfer in favor of BMC of the benefit of any warranties given by such producers or licensors to the Cloud Service Provider.

30. Functional Guarantees

a. The Managed / Cloud Service Provider guarantees that, once the Operational Acceptance Certificate(s) has been issued, the System represents a complete, integrated solution to BMC's requirements set forth in the Technical Requirements and it conforms to all other aspects of the Contract. The Managed / Cloud Service Provider acknowledges that GCC Clause (Commissioning and Operational Acceptance) regarding Commissioning and Operational Acceptance governs how technical conformance of the System to the Contract requirements will be determined.

b. If, for reasons attributable to the Cloud Service Provider, the System does not conform to the Technical Requirements or does not conform to all other aspects of the Contract, the Managed / Cloud Service Provider shall at its cost and expense make such changes, modifications, and/or additions to the System as may be necessary to conform to the Technical Requirements and meet all functional and performance standards. The Managed / Cloud Service Provider shall notify BMC upon completion of the necessary changes, modifications, and/or additions and shall request BMC to repeat the Operational Acceptance Tests until the System achieves Operational Acceptance.

c. If the System (or Subsystem[s]) fails to achieve Operational Acceptance, BMC may consider termination of the Contract, pursuant to GCC Clause (Termination), and forfeiture of the Cloud Service Provider's Performance Security in accordance with GCC Clause (Securities) in compensation for the extra costs and delays likely to result from this failure.

31. Audit, Access and Reporting

a. Purpose

This GCC details the audit, access and reporting rights and obligations of the BMC or its nominated agency and the Cloud Service Provider.

b. **Audit Notice and Timing**

i. As soon as reasonably practicable after the Effective Date, the Parties shall use their best endeavors to agree to a timetable for routine audits during the Project Implementation Phase and the Operation and Management Phase. Such timetable during the Implementation Phase, the BMC or its nominated agency and thereafter during the operation Phase, the BMC or its nominated agency shall conduct routine audits in accordance with such agreed timetable and shall not be required to give the Managed / Cloud Service Provider any further notice of carrying out such audits.

ii. The BMC or its nominated agency may conduct non-timetabled audits at it'sown discretion if it reasonably believes that such non-timetabled audits are necessary as a result of an act of fraud by the Cloud Service Provider, a security violation, or breach of confidentiality obligations by the Cloud Service Provider, provided that the requirement for such an audit is notified in writing to the Managed / Cloud Service Provider a reasonable period time prior to the audit (taking into account the circumstances giving rise to the reasonable belief) stating in a reasonable level of detail the reasons for the requirement and the alleged facts on which the requirement is based.

iii. The frequency of audits shall be a (maximum) half yearly, provided always that the BMC or its nominated agency shall endeavor to conduct such audits with the lowest levels of inconvenience and disturbance practicable being caused to the Cloud Service Provider. Any such audit shall be conducted by with adequate notice of 2 weeks to the Cloud Service Provider.

c. Access

i. The Managed / Cloud Service Provider shall provide to the BMC or its nominated agency reasonable access to employees, subcontractors, Cloud Service Providers, agents and third-party facilities as detailed in the RFB,

documents, records and systems reasonably required for audit and shall provide all such persons with routine assistance in connection with the audits and inspections. The Project Manager of BMC shall have the right to copy and retain copies of any relevant records. The Managed / Cloud Service Provider shall make every reasonable effort to co-operate with them.

d. Audit Rights

i. The BMC or its nominated agency shall have the right to audit and inspect Cloud Service Providers, agents and third party facilities (as detailed in the RFB), data centers, documents, records, procedures and systems relating to the provision of the services, but only to the extent that they relate to the provision of the services, as shall be reasonably necessary to verify:

1. The security, integrity and availability of all data processed, held or conveyed by the Partner on behalf of BMC and documentation related thereto;

2. That the actual level of performance of the services is the same as specified in the Service Level Agreement (SLA);

3. That the Managed / Cloud Service Provider has complied with the relevant technical standards, and has adequate internal controls in place; and

4. The compliance of the Managed / Cloud Service Provider with any other obligation under the Contract and SLA.

5. Security audit and implementation audit of the system shall be done once each year, the cost of which shall be borne by the Cloud Service Provider.

6. For the avoidance of doubt the audit rights under this GCC shall not include access to the Cloud Service Provider's profit margins or overheads, any confidential information relating to the Cloud Service Provider' employees, or (iii) minutes of its internal Board or Board committee meetings including internal audit, or (iv) such other information of commercial-in-confidence nature which are not relevant to the Services associated with any obligation under the Contract.

e. Audit Rights of Sub-contractors, Cloud Service Providers and Agents

i. The Managed / Cloud Service Provider shall use reasonable endeavors to achieve the same audit and access provisions as defined in this GCC with subcontractors who supply labor, services in respect of the services. The Managed / Cloud Service Provider shall inform the BMC or its nominated agency prior to concluding any sub-contract or supply agreement of any failure to achieve the same rights of audit or access.

ii. REPORTING: The Managed / Cloud Service Provider will provide quarterly reports to the Project Manager of BMC, regarding any specific aspects of the Project and in context of the audit and access information as required by the BMC or its nominated agency.

f. Action & Review

i. Any change or amendment to the systems and procedures of the Cloud Service Provider, or sub-contractors, where applicable arising from the audit report shall be agreed within thirty (30) calendar days from the submission of the said report.

ii. Any discrepancies identified by any audit pursuant to this GCC shall be immediately notified to the BMC or its nominated agency and the Managed / Cloud Service Provider Project Manager who shall determine what action

should be taken in respect of such discrepancies in accordance with the terms of the Contract.

g. Terms of Payment

i. The BMC shall bear the cost of any audits and inspections. The terms of payment are exclusive of any costs of the Managed / Cloud Service Provider and the sub-contractor, for all reasonable assistance and information provided under the Contract, the Project Implementation, Operation and Management SLA by the Managed / Cloud Service Provider pursuant to this GCC.

h. Records and Information

i. For the purposes of audit in accordance with this GCC, the Managed / Cloud Service Provider shall maintain true and accurate records in connection with the provision of the services and the Managed / Cloud Service Provider shall handover all the relevant records and documents upon the termination or expiry of the Contract.

32. Intellectual Property Rights Warranty

a. The Managed / Cloud Service Provider hereby represents and warrants that:

i. the System as supplied, installed, tested, and accepted;

ii. use of the System in accordance with the Contract; and

iii. copying of the Software and Materials provided to BMC in accordance with the Contract

iv. 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 BMC to own or exercise all Intellectual Property Rights as provided in the Contract.

v. Pre-existing work: All IPR including the source code and materials developed or otherwise obtained independently of the efforts of a Party under this Agreement (“pre-existing work”) including any enhancement or modification thereto shall remain the sole property of that Party. During the performance of the services for this agreement, each party grants to the other party (and their sub-contractors as necessary) a non-exclusive license to use, reproduce and modify any of its pre-existing work provided to the other party solely for the performance of such services for duration of the Term of this Agreement. Except as may be otherwise explicitly agreed to in a statement of services, upon payment in full, the Managed / Cloud Service Provider should grant BMC a non-exclusive, perpetual, fully paid-up license to use the pre-existing work in the form delivered to BMC as part of the service or deliverables only for its internal business operations. Under such license, either of parties will have no right to sell the pre-existing work of the other party to a Third Party. BMC’s license to pre-existing work is conditioned upon its compliance with the terms of this Agreement and the perpetual license applies solely to the pre-existing work that bidder leaves with BMC at the conclusion of performance of the services.

vi. Residuals: In no event shall Managed / Cloud Service Provider be precluded from independently developing for itself, or for others, anything, whether in tangible or non-tangible form, which is competitive with, or similar to, the deliverables, set-out in this Agreement or Annexure. In addition, subject to the confidentiality obligations, Managed / Cloud Service Provider shall be free to use its general knowledge, skills and experience, and any ideas, concepts,

know-how, and techniques that are acquired or used in the course of providing the Services.

33. Intellectual Property Rights Indemnity

a. The Managed / Cloud Service Provider shall indemnify and hold harmless BMC 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 BMC or its employees or officers may suffer as a result of any infringement or alleged infringement of any Intellectual Property Rights by reason of:

   i. installation of the System by the Managed / Cloud Service Provider or the use of the System, including the Materials, in the country where the site is located;

   ii. copying of the Software and Materials provided the Managed / Cloud Service Provider in accordance with the Agreement; and

   iii. 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 BMC's breach of GCC Clause (Intellectual Property Rights Warranty).

b. 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 Cloud Service Provider, where the infringement arises because of such association or combination and not because of use of the System in its own right.

c. Such indemnities shall also not apply if any claim of infringement:

   i. is asserted by a parent, subsidiary, or affiliate of BMC's organization;

   ii. is a direct result of a design mandated by BMC's Technical Requirements and the possibility of such infringement was duly noted in the Cloud Service Provider's Bid; or

   iii. results from the alteration of the System, including the Materials, by BMC or any persons other than the Managed / Cloud Service Provider or a person authorized by the Cloud Service Provider.

d. If any proceedings are brought or any claim is made against BMC arising out of the matters referred to in GCC Clause (Intellectual Property Rights Indemnity), BMC shall promptly give the Managed / Cloud Service Provider notice of such proceedings or claims, and the Managed / Cloud Service Provider may at its own expense and in BMC's name conduct such proceedings or claim and any negotiations for the settlement of any such proceedings or claim.

   If the Managed / Cloud Service Provider fails to notify BMC within thirty (30) days after receipt of such notice that it intends to conduct any such proceedings or claim, then BMC shall be free to conduct the same on its own behalf. Unless the Managed / Cloud Service Provider has so failed to notify BMC within the thirty (30) days, BMC shall make no admission that may be prejudicial to the defense of any such proceedings or claim. BMC shall, at the Cloud Service Provider's request, afford all available assistance to the Managed / Cloud Service Provider in conducting such proceedings or claim and shall be reimbursed by the Managed / Cloud Service Provider for all reasonable expenses incurred in so doing.

e. BMC shall indemnify and hold harmless the Managed / Cloud Service Provider and its employees, officers, and Subcontractors 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 Managed / Cloud Service Provider or its employees, officers, or Subcontractors 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, drawing, specification, or other documents or materials provided to the Managed / Cloud Service Provider in connection with this Contract by BMC or any persons (other than the Cloud Service Provider) contracted by BMC, except to the extent that such losses, liabilities, and costs arise as a result of the Cloud Service Provider's breach of GCC Clause (Intellectual Property Rights Indemnity).

f. Such indemnity shall not cover

   i. any use of the design, data, drawing, specification, or other documents or materials, other than for the purpose indicated by or to be reasonably inferred from the Contract;

   ii. any infringement resulting from the use of the design, data, drawing, specification, or other documents or materials, or any products produced thereby, in association or combination with any other Goods or Services not provided by BMC or any other person contracted by BMC, 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.

g. Such indemnities shall also not apply:

   i. if any claim of infringement is asserted by a parent, subsidiary, or affiliate of the Cloud Service Provider's organization;

   ii. to the extent that any claim of infringement is caused by the alteration, by the Cloud Service Provider, or any persons contracted by the Cloud Service Provider, of the design, data, drawing, specification, or other documents or materials provided to the Managed / Cloud Service Provider by BMC or any persons contracted by BMC.

h. If any proceedings are brought or any claim is made against the Managed / Cloud Service Provider arising out of the matters referred to in GCC Clause (Intellectual Property Rights Indemnity), the Managed / Cloud Service Provider shall promptly give BMC notice of such proceedings or claims, and BMC may at its own expense and in the Cloud Service Provider's name conduct such proceedings or claim and any negotiations for the settlement of any such proceedings or claim. If BMC fails to notify the Managed / Cloud Service Provider within thirty (30) days after receipt of such notice that it intends to conduct any such proceedings or claim, then the Managed / Cloud Service Provider shall be free to conduct the same on its own behalf. Unless BMC has so failed to notify the Managed / Cloud Service Provider within the thirty (30) days, the Managed / Cloud Service Provider shall make no admission that may be prejudicial to the defense of any such proceedings or claim. The Managed / Cloud Service Provider shall, at BMC's request, afford all available assistance to BMC in conducting such proceedings or claim and shall be reimbursed by BMC for all reasonable expenses incurred in so doing.

34. **Limitation of Liability**

a. Provided the following does not exclude or limit any liabilities of either party in ways not permitted by applicable law:

   i. the Managed / Cloud Service Provider shall not be liable to BMC, 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 Managed / Cloud Service Provider to pay liquidated damages to BMC; and

   ii. the aggregate liability of the Managed / Cloud Service Provider to BMC, whether under the Contract, in tort or otherwise, shall not exceed the total Contract Price, provided that this limitation shall not apply to any obligation of the Managed / Cloud Service Provider to indemnify BMC with respect to intellectual property rights infringement.

35. **Transfer of Ownership**

    a. With the exception of Software and Materials, the ownership of the Information Technologies and other Goods shall be transferred to BMC at the time of Delivery or otherwise under terms that may be agreed upon and specified in the Contract Agreement.

    b. Ownership and the terms of usage of the Software and Materials supplied under the Contract shall be governed by GCC Clause (Copyright) and any elaboration in the Technical Requirements.

    c. Ownership of the Cloud Service Provider's Equipment used by the Managed / Cloud Service Provider and its Subcontractors in connection with the Contract shall remain with the Managed / Cloud Service Provider or its Subcontractors.

36. **Care of the System**

    a. BMC shall become responsible for the care and custody of the System or Subsystems upon their Delivery. BMC shall make good at its own cost any loss or damage that may occur to the System or Subsystems from any cause from the date of Delivery until the date of Operational Acceptance of the System or Subsystems, pursuant to GCC Clause (Commissioning and Operational Acceptance), excepting such loss or damage arising from acts or omissions of the Cloud Service Provider, its employees, or subcontractors.

    b. If any loss or damage occurs to the System or any part of the System by reason of:

        i. (insofar as they relate to the country where the Project Site is located) nuclear reaction, nuclear radiation, radioactive contamination, a pressure wave caused by aircraft or other aerial objects, or any other occurrences that an experienced contractor could not reasonably foresee, or if reasonably foreseeable could not reasonably make provision for or insure against, insofar as such risks are not normally insurable on the insurance market and are mentioned in the general exclusions of the policy of insurance taken out under GCC Clause (Insurances);

        ii. any use not in accordance with the Contract, by BMC or any third party;

        iii. any use of or reliance upon any design, data, or specification provided or designated by or on behalf of BMC, or any such matter for which the Managed / Cloud Service Provider has disclaimed responsibility in accordance with GCC Clause (Design and Engineering),

        BMC shall pay to the Managed / Cloud Service Provider all sums payable in respect of the System or Subsystems that have achieved Operational Acceptance, notwithstanding that the same be lost, destroyed, or damaged. If BMC requests the Managed / Cloud Service Provider in writing to make good any loss or damage to the System thereby occasioned, the Managed / Cloud Service Provider shall make good the same at the cost of BMC in accordance with GCC Clause (Changes to the System). If BMC does not request the Managed / Cloud Service Provider in writing to make good any loss or damage to the System thereby occasioned, BMC shall either request a change in accordance with GCC Clause (Changes to the System), excluding the performance of that part of the System thereby lost, destroyed, or damaged, or, where the loss or damage affects a substantial part of the System, BMC shall terminate the Contract pursuant to GCC Clause (Termination).

    c. BMC shall be liable for any loss of or damage to any Cloud Service Provider's Equipment which BMC has authorized to locate within BMC's premises for use in fulfillment of Cloud Service Provider's obligations under the Contract, except where

such loss or damage arises from acts or omissions of the Cloud Service Provider, its employees, or subcontractors.

37. **Loss of or Damage to Property; Accident or Injury to Workers; Indemnification**

a. The Managed / Cloud Service Provider and each and every Subcontractor shall abide by the job safety, insurance, customs, and immigration measures prevalent and laws in force in India.

b. Subject to GCC Clause (Loss of or Damage to Property; Accident or Injury or Workers; Indemnification), the Managed / Cloud Service Provider shall indemnify and hold harmless BMC 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 BMC 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 Managed / Cloud Service Provider or its Subcontractors, or their employees, officers or agents, except any injury, death, or property damage caused by the negligence of BMC, its contractors, employees, officers, or agents.

c. If any proceedings are brought or any claim is made against BMC that might subject the Managed / Cloud Service Provider to liability under GCC Clause (Loss of or Damage to Property; Accident or Injury or Workers; Indemnification), BMC shall promptly give the Managed / Cloud Service Provider notice of such proceedings or claims, and the Managed / Cloud Service Provider may at its own expense and in BMC's name conduct such proceedings or claim and any negotiations for the settlement of any such proceedings or claim. If the Managed / Cloud Service Provider fails to notify BMC within thirty (30) days after receipt of such notice that it intends to conduct any such proceedings or claim, then BMC shall be free to conduct the same on its own behalf. Unless the Managed / Cloud Service Provider has so failed to notify BMC within the thirty (30) working day period, BMC shall make no admission that may be prejudicial to the defense of any such proceedings or claim. BMC shall, at the Cloud Service Provider's request, afford all available assistance to the Managed / Cloud Service Provider in conducting such proceedings or claim and shall be reimbursed by the Managed / Cloud Service Provider for all reasonable expenses incurred in so doing.

d. BMC shall indemnify and hold harmless the Managed / Cloud Service Provider and its employees, officers, and Subcontractors from any and all losses, liabilities, and costs (including losses, liabilities, and costs incurred in defending a claim alleging such a liability) that the Managed / Cloud Service Provider or its employees, officers, or Subcontractors may suffer as a result of the death or personal injury of any person or loss of or damage to property of BMC, 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 (Insurances), provided that such fire, explosion, or other perils were not caused by any act or failure of the Cloud Service Provider.

e. If any proceedings are brought or any claim is made against the Managed / Cloud Service Provider that might subject BMC to liability under GCC Clause (Loss of or Damage to Property; Accident or Injury or Workers; Indemnification), the Managed / Cloud Service Provider shall promptly give BMC notice of such proceedings or claims, and BMC may at its own expense and in the Cloud Service Provider's name conduct such proceedings or claim and any negotiations for the settlement of any such proceedings or claim. If BMC fails to notify the Managed / Cloud Service Provider within thirty (30) days after receipt of such notice that it intends to conduct any such proceedings or claim, then the Managed / Cloud Service Provider shall be free to conduct the same on its own behalf. Unless BMC has so failed to notify the Managed / Cloud Service Provider within the thirty (30) days, the Managed / Cloud

Service Provider shall make no admission that may be prejudicial to the defense of any such proceedings or claim. The Managed / Cloud Service Provider shall, at BMC's request, afford all available assistance to BMC in conducting such proceedings or claim and shall be reimbursed by BMC for all reasonable expenses incurred in so doing.

f. The party entitled to the benefit of an indemnity under this GCC Clause (Loss of or Damage to Property; Accident or Injury of Workers; Indemnification) 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.

38. **Insurances**

a. The Managed / Cloud Service Provider 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 BMC, who should not unreasonably withhold such approval.

i. Cargo Insurance During Transport

as applicable, 110 percent of the price of the Information Technologies and other Goods in a freely convertible currency, covering the Goods from physical loss or damage during shipment through receipt at the Project Site.

ii. Installation "All Risks" Insurance

as applicable, 110 percent of the price of the Information Technologies and other Goods covering the Goods at the site from all risks of physical loss or damage (excluding only perils commonly excluded under "all risks" insurance policies of this type by reputable insurers) occurring prior to Operational Acceptance of the System.

iii. Third-Party Liability Insurance

The Managed / Cloud Service Provider shall obtain Third-Party Liability Insurance in the amount equal to 110 percent of the price of the Information Technologies, and other Goods, covering bodily injury or death suffered by third parties (including BMC's personnel) and loss of or damage to property (including BMC's property and any Subsystems that have been accepted by BMC) occurring in connection with the supply and provisioning of the Cloud Services. The Insurance shall cover the period from theEffective Date of the Contract till date of Operational Acceptance.

iv. Automobile Liability Insurance

In accordance with the statutory requirements prevailing in India, covering use of all vehicles used by the Managed / Cloud Service Provider or its Subcontractors (whether or not owned by them) in connection with the execution of the Contract.

b. BMC shall be named as co-insured under all insurance policies taken out by the Managed / Cloud Service Provider pursuant to GCC Clause (Insurances), except for the Third-Party Liability, and the Cloud Service Provider's Subcontractors shall be named as co-insured under all insurance policies taken out by the Managed / Cloud Service Provider pursuant to GCC Clause (Insurances) except for Cargo Insurance During Transport. All insurer's rights of subrogation against such co-insured for losses or claims arising out of the performance of the Contract shall be waived under such policies.

c. The Managed / Cloud Service Provider shall deliver to BMC certificates of insurance (or copies of the insurance policies) as evidence that the required policies are in full force and effect.

d. The Managed / Cloud Service Provider shall ensure that, where applicable, its Subcontractor(s) shall take out and maintain in effect adequate insurance policies for their personnel and vehicles and for work executed by them under the Contract, unless such Subcontractors are covered by the policies taken out by the Cloud Service Provider.

e. If the Managed / Cloud Service Provider fails to take out and/or maintain in effect the insurance referred to in GCC Clause (Insurances), BMC may take out and maintain in effect any such insurance and may from time to time deduct from any amount due the Managed / Cloud Service Provider under the Contract any premium that BMC shall have paid to the insurer or may otherwise recover such amount as a debt due from the Cloud Service Provider.

f. Unless otherwise provided in the Contract, the Managed / Cloud Service Provider shall prepare and conduct all and any claims made under the policies affected by it pursuant to this GCC Clause (Insurances), and all monies payable by any insurers shall be paid to the Cloud Service Provider. BMC shall give to the Managed / Cloud Service Provider all such reasonable assistance as may be required by the Managed / Cloud Service Provider in connection with any claim under the relevant insurance policies. With respect to insurance claims in which BMC's interest is involved, the Managed / Cloud Service Provider shall not give any release or make any compromise with the insurer without the prior written consent of BMC. With respect to insurance claims in which the Cloud Service Provider's interest is involved, BMC shall not give any release or make any compromise with the insurer without the prior written consent of the Cloud Service Provider.

39. **Force Majeure**

a. "Force Majeure" shall mean any event beyond the reasonable control of BMC or of the Cloud Service Provider, as the case may be, and which is unavoidable notwithstanding the reasonable care of the party affected and shall include, without limitation, the following:

i. war, hostilities, or warlike operations (whether a state of war be declared or not), invasion, act of foreign enemy, and civil war;

ii. rebellion, revolution, insurrection, mutiny, usurpation of civil or military government, conspiracy, riot, civil commotion, and terrorist acts;

iii. 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;

iv. "strike, sabotage, lockout, embargo, import restriction, port congestion, lack of usual means of public transportation and communication, industrial dispute, shipwreck, shortage or restriction of power supply, epidemics, quarantine, and plague;

v. 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;

vi. failure, by the Cloud Service Provider, to obtain the necessary export permit(s) from the governments of the Country(s) of Origin of the Information Technologies or other Goods, or Cloud Service Provider's Equipment provided that the Managed / Cloud Service Provider 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.

b. 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.

c. 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 (Extension of Time for Achieving Operational Acceptance).

d. 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 fulfill its or their obligations under the Contract, but without prejudice to either party's right to terminate the Contract under GCC Clause (Force Majeure).

e. No delay or nonperformance by either party to this Contract caused by the occurrence of any event of Force Majeure shall:

   i. constitute a default or breach of the Contract;

   ii. (subject to relevant GCC Clauses (Care of the System), (Force Majeure) 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 nonperformance is caused by the occurrence of an event of Force Majeure.

f. 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.

g. In the event of termination pursuant to GCC Clause (Force Majeure), the rights and obligations of BMC and the Managed / Cloud Service Provider shall be as specified in relevant GCC Clauses of (Termination).

h. Notwithstanding GCC Clause (Force Majeure), Force Majeure shall not apply to any obligation of BMC to make payments to the Managed / Cloud Service Provider under this Contract.

40. Risk Purchase Clause

In the event the Managed / Cloud Service Provider fails to execute the project as stipulated in the Contract, or as per the directions given by BMC from time to time, BMC reserves the right to procure similar services from the next eligible Bidder or from alternate sources at the cost of the Cloud Service Provider. Before taking such a decision, BMC shall serve a notice period of one month to the Cloud Service Provider. The 30 day notice period shall be considered as the 'Cure Period' to facilitate the Managed / Cloud Service Provider to cure the breach. The provision for Risk Purchase shall be evoked in the event the Managed / Cloud Service Provider fails to correct the breach within the 'Cure Period'. Further, the Managed / Cloud Service Provider liability to pay shall be set as 25% of the value of the undelivered services.

H. CHANGE IN CONTRACT ELEMENTS

41. **Changes to the System**

a. Introducing a Change

i. Subject to this GCC Clauses (Changes to the System), BMC shall have the right to propose, and subsequently require, the Project Manager to order the Managed / Cloud Service Provider from time to time during the performance of the Contract to make any change, modification, addition, or deletion to, in, or from the System (interchangeably called "Change"), provided that such Change falls within the general scope of the System, does not constitute unrelated work, and is technically practicable, taking into account both the state of advancement of the System and the technical compatibility of the Change envisaged with the nature of the System as originally specified in the Contract.

A Change may involve, but is not restricted to, the substitution of updated Information Technologies and related Services in accordance with GCC Clause (Product Upgrades).

ii. The Managed / Cloud Service Provider may from time to time during its performance of the Contract propose to BMC (with a copy to the Project Manager) any Change that the Managed / Cloud Service Provider considers necessary or desirable to improve the quality or efficiency of the System. BMC may at its discretion approve or reject any Change proposed by the Cloud Service Provider.

iii. Notwithstanding relevant GCC Clauses (Changes to the System), no change made necessary because of any default of the Managed / Cloud Service Provider 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.

iv. The procedure on how to proceed with and execute Changes is specified in these GCC Clauses of (Changes to the System), and further details and sample forms are provided in the Section - Contract Forms in the bidding documents.

v. Moreover, BMC and Managed / Cloud Service Provider will agree, during development of the Project Plan, to a date prior to the scheduled date for Operational Acceptance, after which the Technical Requirements for the System shall be "frozen." Any Change initiated after this time will be dealt with after Operational Acceptance.

b. Changes Originating from BMC

i. If BMC proposes a Change pursuant to GCC Clauses (Changes to the System), it shall send to the Managed / Cloud Service Provider a "Request for Change Proposal," requiring the Managed / Cloud Service Provider to prepare and furnish to the Project Manager as soon as reasonably practicable a "Change Proposal," which shall include the following:

1. brief description of the Change;
2. impact on the Time for Achieving Operational Acceptance;
3. detailed estimated cost of the Change;
4. effect on Functional Guarantees (if any);
5. effect on any other provisions of the Contract.

ii. Upon receipt of the Cloud Service Provider's Change Estimate Proposal, BMC shall do one of the following:

1. accept the Cloud Service Provider's estimate with instructions to the Managed / Cloud Service Provider to proceed with the preparation of the Change Proposal;

2. advise the Managed / Cloud Service Provider of any part of its Change Estimate Proposal that is unacceptable and request the Managed / Cloud Service Provider to review its estimate;
3. advise the Managed / Cloud Service Provider that BMC does not intend to proceed with the Change.

iii. Upon receipt of BMC's instruction to proceed under relevant GCC Clause (Changes to the System), the Managed / Cloud Service Provider shall, with proper expedition, proceed with the preparation of the Change Proposal, in accordance with GCC Clause (Changes to the System). The Cloud Service Provider, at its discretion, may specify a validity period for the Change Proposal, after which if BMC and Managed / Cloud Service Provider has not reached agreement in accordance with GCC Clause (Changes to the System), then BMC shall not intend to proceed with the Change.

iv. The pricing of any Change shall, as far as practicable, be calculated in accordance with the rates and prices included in the Contract. If the nature of the Change is such that the Contract rates and prices are inequitable, the parties to the Contract shall agree on other specific rates to be used for valuing the Change.

v. If before or during the preparation of the Change Proposal it becomes apparent that the aggregate impact of compliance with the Request for Change Proposal and with all other Change Orders that have already become binding upon the Managed / Cloud Service Provider under this GCC Clause (Changes to the System) would be to increase or decrease the Contract Price as originally set forth in Article 2 (Contract Price) of the Contract Agreement by more than fifteen (15) percent, the Managed / Cloud Service Provider may give a written notice of objection to this Request for Change Proposal prior to furnishing the Change Proposal.If BMC accepts the Cloud Service Provider's objection, BMC shall withdraw the proposed Change and shall notify the Managed / Cloud Service Provider in writing of its acceptance.

The Cloud Service Provider's failure to so object to a Request for Change Proposal shall neither affect its right to object to any subsequent requested Changes or Change Orders, nor affect its right to take into account, when making such subsequent objection, the percentage increase or decrease in the Contract Price that any Change not objected to by the Managed / Cloud Service Provider represents.

~~vi.~~ Upon receipt of the Change Proposal, BMC and the Managed / Cloud Service Provider shall mutually agree upon all matters contained in the Change Proposal. Within fourteen (14) days after such agreement, BMC shall, if it intends to proceed with the Change, issue the Managed / Cloud Service Provider a Change Order. If BMC is unable to reach a decision within fourteen (14) days, it shall notify the Managed / Cloud Service Provider with details of when the Managed / Cloud Service Provider can expect a decision. If BMC decides not to proceed with the Change for whatever reason, it shall, within the said period of fourteen (14) days, notify the Managed / Cloud Service Provider accordingly.

vii. If BMC and the Managed / Cloud Service Provider cannot reach agreement on the price for the Change, an equitable adjustment to the Time for Achieving Operational Acceptance, or any other matters identified in the Change Proposal, the Change will not be implemented. However, this provision does not limit the rights of either party under GCC Clause (Settlement of Disputes).

c. Changes Originating from Cloud Service Provider

If the Managed / Cloud Service Provider proposes a Change pursuant to relevant GCC Clause (Changes to the System), the Managed / Cloud Service Provider shall submit to the Project Manager a written "Application for Change Proposal," giving reasons for the proposed Change and including the information specified in the relevant GCC Clause (Changes to the System)1. Upon receipt of the Application for Change Proposal, the parties shall follow the procedures outlined in relevant GCC Clauses (Changes to the System).

42. **Extension of Time for Achieving Operational Acceptance**

a. The time(s) for achieving Operational Acceptance specified in the Schedule of Implementation shall be extended if the Managed / Cloud Service Provider is delayed or impeded in the performance of any of its obligations under the Contract by reason of any of the following:

i. any Change in the System as provided in GCC Clause (Change in the System);

ii. any occurrence of Force Majeure as provided in GCC Clause (Force Majeure);

iii. default of BMC; or

iv. 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 Cloud Service Provider.

b. Except where otherwise specifically provided in the Contract, the Managed / Cloud Service Provider 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, BMC and the Managed / Cloud Service Provider shall agree upon the period of such extension. In the event that the Managed / Cloud Service Provider does not accept BMC's estimate of a fair and reasonable time extension, the Managed / Cloud Service Provider shall be entitled to refer the matter to the provisions for the Settlement of Disputes pursuant to GCC Clause (Fraud and Corruption).

c. The Managed / Cloud Service Provider shall at all times use its reasonable efforts to minimize any delay in the performance of its obligations under the Contract.

43. **Termination**

a. Termination for BMC's Convenience

i. BMC may at any time terminate the Contract for any reason by giving the Managed / Cloud Service Provider a notice of termination that refers to this GCC Clause (Termination).

ii. Upon receipt of the notice of termination under this GCC Clause (Termination), the Managed / Cloud Service Provider shall either as soon as reasonably practical or upon the date specified in the notice of termination

1. cease all further work, except for such work as BMC may specify in the notice of termination for the sole purpose of protecting that part of the System already executed, or any work required to leave the site in a clean and safe condition;

2. terminate all subcontracts, except those to be assigned to BMC pursuant to this GCC Clause (Termination) (ii) below;

3. remove all Cloud Service Provider's Equipment from the site, repatriate the Cloud Service Provider's and its Subcontractors' personnel from the site, remove from the site any wreckage, rubbish, and debris of any kind;
4. in addition, the Cloud Service Provider, subject to the payment specified in this GCC Clause (Termination), shall
    a. deliver to BMC the parts of the System executed by the Managed / Cloud Service Provider up to the date of termination;
    b. to the extent legally possible, assign to BMC all right, title, and benefit of the Managed / Cloud Service Provider to the System, or Subsystem, as at the date of termination, and, as may be required by BMC, in any subcontracts concluded between the Managed / Cloud Service Provider and its Subcontractors;
    c. deliver to BMC all nonproprietary drawings, specifications, and other documents prepared by the Managed / Cloud Service Provider or its Subcontractors as of the date of termination in connection with the System.

iii. In the event of termination of the Contract under this GCC Clause (Termination), BMC shall pay to the Managed / Cloud Service Provider the following amounts:

1. the Contract Price, properly attributable to the parts of the System executed by the Managed / Cloud Service Provider as of the date of termination;

b. Termination for Cloud Service Provider's Default

i. BMC, without prejudice to any other rights or remedies it may possess, may terminate the Contract forthwith in the following circumstances by giving a notice of termination and its reasons therefore to the Cloud Service Provider, referring to this GCC Clause (Termination):

1. if the Managed / Cloud Service Provider becomes bankrupt or insolvent, has a receiving order issued against it, compounds with its creditors, or, if the Managed / Cloud Service Provider is a corporation, a resolution is passed or order is made for its winding up (other than a voluntary liquidation for the purposes of amalgamation or reconstruction), a receiver is appointed over any part of its undertaking or assets, or if the Managed / Cloud Service Provider takes or suffers any other analogous action in consequence of debt;
2. if the Managed / Cloud Service Provider assigns or transfers the Contract or any right or interest therein in violation of the provision of GCC Clause (Assignment); or

ii. If the Cloud Service Provider:

1. has abandoned or repudiated the Contract;
2. has without valid reason failed to commence work on the System promptly;
3. persistently fails to execute the Contract in accordance with the provisions of the Contract or persistently neglects to carry out its obligations under the Contract without just cause;
4. refuses or is unable to provide sufficient Materials, Services, or labor to execute and complete the System in the manner specified in the Agreed Project Plan furnished under GCC Clause (Project Plan) at

rates of progress that give reasonable assurance to BMC that the Managed / Cloud Service Provider can attain Operational Acceptance of the System by the Time for Achieving Operational Acceptance as extended;

then BMC may, without prejudice to any other rights it may possess under the Contract, give a notice to the Managed / Cloud Service Provider stating the nature of the default and requiring the Managed / Cloud Service Provider to remedy the same. If the Managed / Cloud Service Provider fails to remedy or to take steps to remedy the same within fourteen (14) days of its receipt of such notice, then BMC may terminate the Contract forthwith by giving a notice of termination to the Managed / Cloud Service Provider that refers to this GCC Clause (Termination).

iii. Upon receipt of the notice of termination under GCC Clauses (Termination), the Managed / Cloud Service Provider shall, either immediately or upon such date as is specified in the notice of termination:

1. cease all further work, except for such work as BMC may specify in the notice of termination for the sole purpose of protecting that part of the System already executed or any work required to leave the site in a clean and safe condition;
2. terminate all subcontracts, except those to be assigned to BMC pursuant to GCC Clause (Termination) below;
3. deliver to BMC the parts of the System executed by the Managed / Cloud Service Provider up to the date of termination;
4. to the extent legally possible, assign to BMC all right, title and benefit of the Managed / Cloud Service Provider to the System or Subsystems as at the date of termination, and, as may be required by BMC, in any subcontracts concluded between the Managed / Cloud Service Provider and its Subcontractors;
5. deliver to BMC all drawings, specifications, and other documents prepared by the Managed / Cloud Service Provider or its Subcontractors as at the date of termination in connection with the System.

iv. BMC may enter upon the site, expel the Cloud Service Provider, and complete the System itself or by employing any third party. Upon completion of the System or at such earlier date as BMC thinks appropriate, BMC shall give notice to the Managed / Cloud Service Provider that such Cloud Service Provider's Equipment will be returned to the Managed / Cloud Service Provider at or near the site and shall return such Cloud Service Provider's Equipment to the Managed / Cloud Service Provider in accordance with such notice. The Managed / Cloud Service Provider shall thereafter without delay and at its cost remove or arrange removal of the same from the site.

v. Subject to GCC Clause (Termination), the Managed / Cloud Service Provider shall be entitled to be paid the Contract Price attributable to the portion of the System executed as at the date of termination and the costs, if any, incurred in protecting the System and in leaving the site in a clean and safe condition pursuant to GCC Clause (Termination). Any sums due BMC from the Managed / Cloud Service Provider accruing prior to the date of termination shall be deducted from the amount to be paid to the Managed / Cloud Service Provider under this Contract.

vi. If BMC completes the System, the cost of completing the System by BMC shall be determined. If the sum that the Managed / Cloud Service Provider is entitled to be paid, pursuant to GCC Clause (Termination), plus the

reasonable costs incurred by BMC in completing the System, exceeds the Contract Price, the Managed / Cloud Service Provider shall be liable for such excess. If such excess is greater than the sums due the Managed / Cloud Service Provider under GCC Clause (Termination), the Managed / Cloud Service Provider shall pay the balance to BMC, and if such excess is less than the sums due the Managed / Cloud Service Provider under GCC Clause (Termination), BMC shall pay the balance to the Cloud Service Provider. BMC and the Managed / Cloud Service Provider shall agree, in writing, on the computation described above and the manner in which any sums shall be paid.

c. In this GCC Clause (Termination), the expression "portion of the System executed" shall include all work executed, Services provided, and all Information Technologies, or other Goods acquired (or subject to a legally binding obligation to purchase) by the Managed / Cloud Service Provider and used or intended to be used for the purpose of the System, up to and including the date of termination.

d. In this GCC Clause (Termination), in calculating any monies due from BMC to the Cloud Service Provider, account shall be taken of any sum previously paid by BMC to the Managed / Cloud Service Provider under the Contract, including any advance payment paid.

44. Exit Management

a. **Purpose**

i. This GCC sets out the provisions, which will apply on expiry or termination of the Contract, the Project Implementation, Operation and Management Service Level Agreement (SLA).

ii. In the case of termination of the Project Implementation and/or Operation and Management, the Parties shall agree at that time whether, and if so during what period, the provisions of this GCC shall apply.

iii. The Parties shall ensure that their respective associated entities carry out their respective obligations set out in this GCC (Exit Management).

b. Transfer of Assets

i. BMC shall be entitled to serve notice in writing on the Managed / Cloud Service Provider at any time during the exit management period as detailed hereinabove requiring the Managed / Cloud Service Provider and/or its sub-contractors to provide the BMC with a complete and up to date list of the Assets within 30 days of such notice. BMC shall then be entitled to serve notice in writing on the Managed / Cloud Service Provider at any time prior to a date that is 30 days prior to the end of the exit management period requiring the Managed / Cloud Service Provider to sell the Assets (if any), to be transferred to BMC or its nominated agencies at book value as determined as of the date of such notice in accordance with the provisions of relevant laws.

ii. In case of contract being terminated by BMC, BMC reserves the right to ask Managed / Cloud Service Provider to continue running the project operations for a period of 6 months after termination orders are issued.

iii. Upon service of a notice under this GCC, the following provisions shall apply:

1. in the event, if the Assets to be transferred are mortgaged to any financial institutions by the Cloud Service Provider, the Managed / Cloud Service Provider shall ensure that all such liens and liabilities have been cleared beyond doubt, prior to such transfer. All documents regarding the discharge of such lien and liabilities shall be furnished to the BMC.

2. All risk in and title to the Assets to be transferred / to be purchased by the BMC pursuant to this GCC shall be transferred to BMC, on the last day of the exit management period.
3. BMC shall pay to the Managed / Cloud Service Provider on the last day of the exit management period such sum representing the Net Block (procurement price less depreciation as per provisions of Companies Act) of the Assets to be transferred as stated in the Terms of Payment Schedule, if any.
4. Payment to the outgoing Managed / Cloud Service Provider shall be made to the tune of the last set of completed services / deliverables, subject to SLA requirements.
5. The outgoing Managed / Cloud Service Provider will pass on to BMC and/or to the Replacement Cloud Service Provider, the subsisting rights in any leased properties/ licensed products on terms not less favorable to BMC/ Replacement Cloud Service Provider, than that enjoyed by the outgoing Cloud Service Provider.

c. Cooperation and Provision of Information

i. During the exit management period:

1. The Managed / Cloud Service Provider will allow the BMC or its nominated agency access to information reasonably required to define the then current mode of operation associated with the provision of the services to enable the BMC to assess the existing services being delivered;
2. promptly on reasonable request by the BMC, the Managed / Cloud Service Provider shall provide access to and copies of all information held or controlled by them which the Managed / Cloud Service Provider have prepared or maintained in accordance with the contract, relating to any material aspect of the services (whether provided by the Managed / Cloud Service Provider or sub-contractors appointed by the Cloud Service Provider). The BMC shall be entitled to a copy of all such information. Such information shall include details pertaining to the services rendered and other performance data. The Managed / Cloud Service Provider shall permit the BMC or its nominated agencies to have reasonable access to its employees and facilities as reasonably required to understand the methods of delivery of the services employed by the Managed / Cloud Service Provider and to assist appropriate knowledge transfer.

d. Confidential Information, Security and Data

i. The Managed / Cloud Service Provider will promptly on the commencement of the exit management period supply to the BMC or its nominated agency the following:

1. information relating to the current services rendered to the citizens / customer and performance data relating to the performance of sub-contractors in relation to the services;
2. documentation relating to Cloud Services Project's Intellectual Property Rights;
3. documentation relating to sub-contractors;
4. all current and updated data as is reasonably required for purposes of BMC or its nominated agencies transitioning the services to its Replacement Managed / Cloud Service Provider in a readily available format nominated by the BMC or its nominated agency;
5. all other information (including but not limited to documents, records and agreements) relating to the services reasonably necessary to enable BMC or its nominated agencies, or its Replacement Managed

/ Cloud Service Provider to carry out due diligence in order to transition the provision of the Services to BMC or its nominated agencies, or its Replacement Managed / Cloud Service Provider (as the case may be)

ii. Before the expiry of the exit management period, the Managed / Cloud Service Provider shall deliver to the BMC or its nominated agency all new or up-dated materials from the categories set out in the Contract and shall not retain any copies thereof, except that the Managed / Cloud Service Provider shall be permitted to retain one copy of such materials for archival purposes only.

iii. Before the expiry of the exit management period, unless otherwise provided under the Contract, the BMC or its nominated agency shall deliver to the Managed / Cloud Service Provider all forms of Cloud Service Providers confidential information, which is in the possession or control of BMC.

e. Employees

i. Promptly on reasonable request at any time during the exit management period, the Cloud Service Providers shall, subject to applicable laws, restraints and regulations (including in particular those relating to privacy) provide to the BMC or its nominated agency a list of all employees (with job titles) of the Managed / Cloud Service Provider dedicated to providing the services at the commencement of the exit management period.

ii. Where any national, regional law or regulation relating to the mandatory or automatic transfer of the contracts of employment from the Managed / Cloud Service Provider to the BMC or its nominated agency, or a Replacement Managed / Cloud Service Provider ("Transfer Regulation") applies to any or all of the employees of the Managed / Cloud Service Provider then the Parties shall comply with their respective obligations under such Transfer Regulations.

f. Transfer of Certain Agreements

On request by the BMC or its nominated agency, the Managed / Cloud Service Provider shall effect such assignments, transfers, licences and sub-licences as the Project Manager of BMC may require in favour of the BMC or its Replacement Managed / Cloud Service Provider in relation to any equipment lease, maintenance or service provision agreement between Managed / Cloud Service Provider and third party lessors, vendors, and which are related to the services and reasonably necessary for the carrying out of replacement services by the BMC or its nominated agency or its Replacement Cloud Service Provider.

g. Rights of Access to Premises

i. At any time during the exit management period, where Assets are located at the Cloud Service Provider's premises, the Managed / Cloud Service Provider will be obliged to give reasonable rights of access to (or, in the case of Assets located on a third party's premises, procure reasonable rights of access to) the BMC or its nominated agency and/or any Replacement Managed / Cloud Service Provider in order to make an inventory of the Assets.

ii. The Managed / Cloud Service Provider shall also give the BMC or its nominated agency or its nominated agencies, or any Replacement Managed / Cloud Service Provider right of reasonable access to the Implementation Partner's premises and shall procure the BMC or its nominated agency or its nominated agencies and any Replacement Managed / Cloud Service Provider rights of access to relevant third party premises during the exit management period and for such period of time following termination or expiry of the CONTRACT as is reasonably necessary to migrate the services

to the BMC or its nominated agency, or a Replacement Cloud Service Provider.

h. **General Obligations of the Cloud Service Provider**

i. The Managed / Cloud Service Provider shall provide all such information as may reasonably be necessary to effect as seamless a handover as practicable in the circumstances to the BMC or its nominated agency or its Replacement Managed / Cloud Service Provider and which the Managed / Cloud Service Provider has in its possession or control at any time during the exit management period.

ii. For the purposes of this GCC, anything in the possession or control of any Cloud Service Provider, associated entity, or sub-contractor is deemed to be in the possession or control of the Cloud Service Provider.

iii. The Managed / Cloud Service Provider shall commit adequate resources to comply with its obligations under this Exit Management GCC.

i. Exit Management Plan

i. The Managed / Cloud Service Provider shall provide the BMC or its nominated agency with a recommended exit management plan ("Exit Management Plan") which shall deal with at least the following aspects of exit management in relation to the CONTRACT as a whole and in relation to the Project Implementation, and the Operation and Management SLA.

1. A detailed program of the transfer process that could be used in conjunction with a Replacement Managed / Cloud Service Provider including details of the means to be used to ensure continuing provision of the services throughout the transfer process or until the cessation of the services and of the management structure to be used during the transfer;

2. plans for the communication with such of the Cloud Service Provider's sub contractors, staff, Cloud Service Providers, customers and any related third party as are necessary to avoid any material detrimental impact on the BMC's operations as a result of undertaking the transfer;

3. (if applicable) proposed arrangements for the segregation of the Cloud Service Provider's networks from the networks employed by BMC and identification of specific security tasks necessary at termination;

4. Plans for provision of contingent support to BMC, and Replacement Managed / Cloud Service Provider for a reasonable period after transfer.

ii. The Managed / Cloud Service Provider shall re-draft the Exit Management Plan annually thereafter to ensure that it is kept relevant and up to date.

iii. Each Exit Management Plan shall be presented by the Managed / Cloud Service Provider to and approved by the BMC or its nominated agencies.

iv. The terms of payment as stated in the Terms of Payment Schedule include the costs of the Managed / Cloud Service Provider complying with its obligations under this GCC.

v. In the event of termination or expiry of CONTRACT, and Project Implementation, each Party shall comply with the Exit Management Plan.

vi. During the exit management period, the Managed / Cloud Service Provider shall use its best efforts to deliver the services

vii. Payments during the Exit Management period shall be made in accordance with the Terms of Payment Schedule.

viii. This Exit Management plan shall be furnished in writing to the BMC or its nominated agencies within 90 days from the Effective Date of this Contract**.**

45. Assignment

a. Neither BMC nor the Managed / Cloud Service Provider shall, without the express prior written consent of the other, assign to any third party the Contract or any part thereof, or any right, benefit, obligation, or interest therein or thereunder, except that the Managed / Cloud Service Provider shall be entitled to assign either absolutely or by way of charge any monies due and payable to it or that may become due and payable to it under the Contract.

46. **Settlement of Disputes**

a. Adjudication

i. If any dispute of any kind whatsoever shall arise between BMC and the Managed / Cloud Service Provider in connection with or arising out of the Contract, including without prejudice to the generality of the foregoing, any question regarding its existence, validity, or termination, or the operation of the System (whether during the progress of implementation or after its achieving Operational Acceptance and whether before or after the termination, abandonment, or breach of the Contract), the parties shall seek to resolve any such dispute by mutual consultation. If the parties fail to resolve such a dispute by mutual consultation within fourteen (14) days after one party has notified the other in writing of the dispute, then, if the Contract Agreement in Appendix 2 includes and names an Adjudicator, the dispute shall, within another fourteen (14) days, be referred in writing by either party to the Adjudicator, with a copy to the other party. If there is no Adjudicator specified in the Contract Agreement, the mutual consultation period stated above shall last thirty (30) days (instead of fourteen), upon expiry of which either party may move to the notification of arbitration pursuant to this GCC Clause (Settlement of Disputes).

ii. The Adjudicator shall give his or her decision in writing to both parties within thirty (30) days of the dispute being referred to the Adjudicator. If the Adjudicator has done so, and no notice of intention to commence arbitration has been given by either BMC or the Managed / Cloud Service Provider within fifty-six (56) days of such reference, the decision shall become final and binding upon BMC and the Cloud Service Provider. Any decision that has become final and binding shall be implemented by the parties forthwith.

b. Arbitration

i. If

1. BMC or the Managed / Cloud Service Provider is dissatisfied with the Adjudicator's decision and acts before this decision has become final and binding pursuant to GCC Clause (Settlement of Disputes), or

2. the Adjudicator fails to give a decision within the allotted time from referral of the dispute pursuant to GCC Clause (Settlement of Disputes), and BMC or the Managed / Cloud Service Provider acts within the following fourteen (14) days, or

3. in the absence of an Adjudicator from the Contract Agreement, the mutual consultation pursuant to GCC Clause (Settlement of Disputes) expires without resolution of the dispute and BMC or the Managed / Cloud Service Provider acts within the following fourteen (14) days,

then either BMC or the Managed / Cloud Service Provider may act to give notice to the other party, with a copy for information to the Adjudicator in case an Adjudicator had been involved, of its intention to commence arbitration, as provided below, as to the matter in dispute, and no arbitration in respect of this matter may be commenced unless such notice is given.

ii. Any dispute in respect of which a notice of intention to commence arbitration has been given, in accordance with GCC Clause (Settlement of Disputes), shall be finally settled by arbitration. Arbitration may be commenced prior to or after provisioning of the Cloud Services.

iii. Arbitration proceedings shall be conducted in accordance with the provisions of the Arbitration Act, 1996.

c. Notwithstanding any reference to the Adjudicator or arbitration in this clause,

i. the parties shall continue to perform their respective obligations under the Contract unless they otherwise agree;

ii. BMC shall pay the Managed / Cloud Service Provider any monies due the Cloud Service Provider.