# Request for Proposal

# For

# Hiring of "Cloud based Disaster Recovery Services" from Managed Service Provider at Mumbai Metro Rail Corporation

**Tender Reference Number: MMRC/IT/RFP DC-DR/71**

**Date of Issue: 22.09.2017**

**Tender document Amount: Rs. 5000/-**

**Issued By:**

**Executive Director (Electrical)**
**5th Floor, MMRDA Old Building**
**Bandra Kurla Complex**
**Bandra (East)**
**Mumbai 400 051**
**Email**: itpmo.mmrc@gmail.com

## Table of Contents

# 1. Disclaimer

This Request for Proposal (**RFP**) for "**Hiring of "Cloud based Disaster Recovery Services" from Managed Service Provider at Mumbai Metro Rail Corporation (MMRC)"** is issued by Mumbai Metro Rail Corporation (MMRC)**.**

Whilst the information in this RFP has been prepared in good faith, it is not and does not purport to be comprehensive or to have been independently verified. Neither MMRC, nor any of its officers or employees, nor any of their advisers nor consultants accept any liability or responsibility for the accuracy, reasonableness or completeness of the information contained in the RFP, or for any errors, omissions or misstatements, negligent or otherwise, relating to the proposed Hiring of "Cloud based Disaster Recovery Services" from Managed Service Provider at Mumbai Metro Rail Corporation (MMRC) (hereinafter referred to as "MMRC Cloud Based DR"), or makes any representation or warranty, express or implied, with respect to the information contained in this RFP or on which this RFP is based or with respect to any written or oral information made or to be made available to any of the recipients or their professional advisers and, so far as permitted by law and except in the case of fraudulent misrepresentation by the party concerned, and liability therefore is hereby expressly disclaimed.

The information contained in this RFP is selective and is subject to updating, expansion, revision and amendment at the sole discretion of MMRC. It does not, and does not purport to, contain all the information that a recipient may require for the purposes for making a decision for participation in this process. Each party must conduct its own analysis of the information contained in this RFP, to correct any inaccuracies therein and is advised to carry out its own investigation into the proposed MMRC Project, the regulatory regime which applies thereto and by and all matters pertinent to the MMRC Project and to seek its own professional advice on the legal, financial and regulatory consequences of entering into any agreement or arrangement relating to the MMRC Project. MMRC shall not be responsible for any direct or indirect loss or damage arising out of or for use of any content of the RFP in any manner whatsoever.

MMRC shall be the sole and final authority with respect to qualifying a bidder through this RFP. The decision of MMRC in selecting the Service Provider who qualifies through this RFP shall be final and MMRC reserves the right to reject any or all the bids without assigning any reason thereof. MMRC further reserves the right to negotiate with the selected Service Provider (SP) to enhance the value through this project and to create a more amicable environment for the smooth execution of the project.

MMRC may terminate the RFP process at any time without assigning any reason and upon such termination MMRC shall not be responsible for any direct or indirect loss or damage arising out of such a termination.

## 1.1 Abbreviations

| Abbreviation | Description |
|---|---|
| **B2C** | Business to Consumer |
| **BI** | Business Intelligence |
| **BKC** | Bandra Kurla Complex |
| **CMMI** | Capability Maturity Model Integration |
| **DC** | Data Centre |
| **DEV** | Development |
| **DR** | Disaster Recovery |
| **DSC** | Digital Signal Certificate |
| **EMD** | Earnest Money Deposit |
| **ETIM** | Electronic Ticketing Machine |
| **GCC** | General Contract Conditions |
| **GoM** | Government of Maharashtra |
| **ICT** | Information Communication Technology |
| **IT** | Information Technology |
| **ITB** | Instructions to bidder |
| **MIS** | Management Information System |
| **MML-3** | Mumbai Metro Line – 3 |
| **MMRC** | Mumbai Metro Rail Corporation |
| **MSP** | Managed Service Provider |
| **NDA** | Non-Disclosure Agreement |
| **NIC** | National Informatics Centre |
| **PBG** | Performance Bank Guarantee |
| **PDF** | Portable Document Format |
| **PM** | Project Management |
| **QGR** | Quarterly Guaranteed Revenue |
| **RFP** | Request for Proposal |
| **RFP** | Request for Proposal |
| **SD** | Security Deposit |
| **SLA** | Service Level Agreement |
| **TEC** | Tender Evaluation Committee |

## 1.2 Key Terms – Definition

| Term | Definition |
|---|---|
| Bid / Proposal | This means the documents in their entirety comprising of the pre-qualification Proposal, Technical and Commercial Proposal, clarifications to these, technical presentation/ demo submitted by the Bidder, the Bidder herein, in response to the RFP, and accepted by MMRC. |
| Bidder(s) | Eligible, reputed, qualified IT entities or Consortium of these with strong technical and financial capabilities for supply, design, customization, implementation, hosting and maintenance of ICT Solution who may be responding to this RFP. |
| Bidder's Representative | The person or the persons appointed by the Bidder from time to time to act on its behalf for overall co-ordination, supervision and execution of Project. |
| Business Day | This means any day that is not a Sunday or a public holiday (as declared by Government of Maharashtra). |
| Contract / Project Period | 5 Years post Go-Live. |
| Day | A period of 24 hours running from midnight to midnight. It means "calendar day" unless otherwise stated. Where, because of a difference in time zone, the calendar day in one country differs from another country then the calendar day shall be deemed to be the calendar day applicable to India. |
| Deliverables | The documents, milestones and activities related to the setting up and operations of Project in MMRC, as defined in the RFP. |
| EMD/ Bid Security | This refers to the amount to be deposited by the Bidders to MMRC to demonstrate commitment and intention to complete the process of selection of Bidder for implementation of ERP in MMRC. |
| End of Contract | This refers to the time when the Contract Period has ended. |
| RFP/ Tender | This means the Request for Proposal released, containing the technical, functional, commercial and operational specification. |
| Contract | This shall mean the deed to contract, together with its original accompaniment and those latter incorporated in it by mutual consent. |
| Contractor | This shall mean the successful Bidder whose tender has been accepted, and who has been authorized to proceed with the Work. |
| Subcontractor | This means person or corporate body who has a Contract with the Contractor to carry out a part of the Work in the Contract which includes work on the Site. |
| Employer | This shall mean MMRC and is the party who will employ the Contractor to carry out the Works. |
| Users | This means the internal and external users of the System including citizens, business firms, MMRC including its offices, corporations and agencies and their employees, as the context admits or requires |

## 1.3 Tender Notice

**TENDER NOTICE**

**Tender Reference No: MMRC/IT/RFP DC-DR/71** **Date: - 22.09.2017**

Mumbai Metro Rail Corporation (MMRC) hereby invites bids from eligible bidders for Hiring of "Cloud based Disaster Recovery services" from Managed Service Provider at Mumbai Metro Rail Corporation (MMRC). Last date for bid submission is 07.11.2017 till 6:00 pm & EMD amount will be Rs. 2, 20, 000/- (Rupees Two Lakhs Twenty Thousand Only). For details, please refer e-tendering portal www.tenderwizard.com/MMRC & for any e-Tendering support, bidder may contact ITI representative at (Ph. No. 7666563870/8013426317) for any assistance. Contact Timings-India 09.00 Hrs. – 20.00Hrs (GMT+5.30).

Date : 22.09.2017
Place : Mumbai

SD
Executive Director (Electrical)/ IT
Incharge, MMRC

## 2. Invitation for Proposal

MMRC hereby invites Proposals from reputed, competent and professional companies, who meet the Pre-Qualification Criteria as specified in this bidding document for **"Hiring of "Cloud based Disaster Recovery services" from Managed Service Provider at Mumbai Metro Rail Corporation (MMRC)"** as detailed in Section 3.23 of this RFP document.

All documents related to RFP is available from the MMRC e-tendering portal www.tenderwizard.com/MMRC, without registration. All bidders must note that this being E-tender, bids received only through online on E-tendering portal www.tenderwizard.com/MMRC shall be considered as an offer. Any bid submitted in paper form will not be received and opened and shall be summarily rejected. To participate applicant / bidders is required to register and bid using following steps.

**Step 1: Registration of Applicants/Bidders**

- Go to website: www.tenderwizard.com/MMRC.
- Click on "Register Me" button.
- Fill in their desired User ID, Company Details by their own.
- Vendor in possession of DSC Class III may insert Digital Signature Certificate token in computer's USB drive, and click on "Update Digital Signing Certificate Serial No. From USB token". A new PKI based Signer Certificate" window will open. Browse your Signer Certificate, enter token password and click on Register.
- For those without DSC, it is mandatory to apply for the DSC.
- Do not enter special character(s) in any field except "Email Address", "Website (URL)" and "Alternative Email Address".
- Then click on "Create profile".
- You will be forwarded to "Document Upload" screen. Upload documents as specified in previous page. After uploading is completed, click on "Finish Upload".
- You will be forwarded to Payment screen. Make registration payment.
- The User ID and system generated password with payment confirmation will appear on the next screen which can be printed for future reference.
- For enabling the User ID, forward the registration acknowledgement to twhelpdesk680@gmail.com and twhelpdesk753@gmail.com along with a Request Letter.
- Download the format for Request letter from Home page (available under Click to view Latest Circulars / Format). Letter should be duly signed with rubber stamp.

**Step 2: Apply digital signature (known as "digital signature certificate"): following registration a token (data card) will be issued to the registered company.**

- **Applying Class III Digital Signature Certificate: (token issued upon registration)**

- The applicant/bidder is required to apply for a class III Digital Signature Certificate (DSC). Digital Signature Certificate which is obtainable from either the authorized agencies of CCA (Controller of Certifying Authorities in India www.cca.gov.in).
- **Procedure for submission of E-tender by bidder:**
- Interested bidders who wish to participate should visit website http://www.tenderwizard.com/MMRC which is the ONLY website for bidding their offer. Further, the procedure is as follows:
- Register your company in website www.tenderwizard.com/MMRC for obtaining a Login ID and Password (after paying necessary registration charges). This is one time annual payment and applicable for bidding other tenders also**.**
- Using the login ID, password and digital signature, enter the tender portal to purchase the tender document.
- Pay processing fees and tender cost through e-payment gateway.
- With the payment of processing fee and tender cost, the bidder can download the 'Technical bid' (Microsoft Excel file 'Technicalbid.xls') and 'Financial bid' (Microsoft Excel file 'Financialbid.xls') by clicking on the link "Show Form".
- Download the 'Technical bid' and 'Financial bid' and save them without changing the file name. Fill up your quotations, save them. Then upload the 'Technical bid' and 'Financial bid' in appropriate links.
- Attach supporting documents first in "Document Library". Then attach them by selecting in particular tender.
- Submit your tender. You will receive a system generated "Acknowledgement Copy" of tender submission.
- Bidder can change quoted rates any time before of closing date & time.
- Bidder must submit the offer before the online closing date & time. The website will automatically stop accepting the offer after online closing date and time.
- Bidder manual & system requirement is available on website www.tenderwizard.com/MMRC for necessary help.
- All Bids must be uploaded on-line on E-Tendering portal. www.tenderwizard.com/MMRC before the time and date specified in the pre-qualification Data sheet / Bid Data sheet.
- Being e-tenders the bidders will not be able to upload bids after the designated time of bid submission.
- The Applicants/Bidders are advised to keep in touch with the e-tendering portal www.tenderwizard.com/MMRC for updates.
- N.B: Bidders are requested to refer to the Vendor's manual by downloading the Vendor's Manual by visiting www.tenderwizard.com/MMRC and clicking on "Help Manuals".

- Bidder may contact ITI representative at (Ph. No. 011 49424365) for any assistance. Contact Timings-India 09.00 Hrs. – 20.00Hrs (GMT +5.30)

Bidder/ Agencies are advised to study this RFP document carefully before submitting their proposals in response to the RFP Notice. Submission of a proposal in response to this notice shall be deemed to have been done after careful study and examination of this document with full understanding of its terms, conditions and implications. Prospective bidders are advised to check the minimum qualification criteria before participating in the bidding process. This RFP document is not transferable and the name of the bidder who purchases and submits the same bid shall be unchanged.

## 2.1 Key Events and Dates

The summary of various activities with regard to this invitation of bids are listed in the table below:-

| # | Particular | Details |
|---|---|---|
| 1. | Advertising Date | From: 22.09.2017, Time : 11:00 am |
| 2. | Name of the project | RFP for "Hiring of "Cloud based Disaster Recovery services" from Managed Service Provider at Mumbai Metro Rail Corporation (MMRC)" |
| 3. | RFP Document Download and Submission Start Date & Time | From Date: 22.09.2017, Time : 11:00 am<br>Till Date: 07.11.2017, Time : 6:00 pm |
| 4. | Website for downloading Tender Document, Corrigendum's, Addendums etc. | www.tenderwizard.com/MMRC |
| 5. | Last date for Submission of Queries | 29.09.2017 at 6:00 pm<br>All the queries should be received on or before, through email only with subject line as follows:<br>"Pre-Bid queries - <Agency's Name>".<br>The queries should be submitted as per the format prescribed in section 6.3.<br>The Pre-Bid queries to be sent to the Email Id – itpmo.mmrc@gmail.com |
| 6. | Pre-Bid Conference | 05.10.2017 at 3:00 pm<br>**Address:** 6th Floor,<br>MMRDA Old Building |

| | | |
|---|---|---|
| | | Bandra Kurla Complex<br>Bandra (East)<br>Mumbai—400 051 |
| 7. | Last date (deadline) for Submission of bids | 07.11.2017 till 6.00 pm |
| 8. | Date and time of opening of Technical Bid Opening | 08.11.2017 at 11:00 am |
| 9. | Date and time for opening of Commercial bids | Will be intimated later to the qualified bidders |
| 10. | Detail of the contact person and Address at which sealed bids are to be submitted | Shri. R. K Sharma,<br>Executive Director (Electrical)<br>5th Floor, MMRDA Old Building<br>Bandra Kurla Complex<br>Bandra (East)<br>Mumbai—400 051<br>E-mail: itpmo.mmrc@gmail.com |

## 2.2 Other Important Information Related to Bid

| #. | Item | Description |
|---|---|---|
| 1. | Earnest Money Deposit (EMD) - Online | Rs. 2,20,000/- (Rupees Two Lakhs Twenty Thousand Only) |
| 2. | RFP Document Fee to be paid via Online Payment Gateway mode only. | Rs. 5000 (Rupees Five Thousand Only) |
| 3. | Bid Validity Period | One hundred and eighty (180) days from the date of opening of bid |
| 4. | Performance Security Deposit value (Bank Guarantee)<br>Last date for furnishing Performance Security Deposit to MMRC (By successful bidder) | 10% of total contract value of successful bidder<br>To be submitted within fourteen (14) working days of the date of notice of award of the contract or prior to signing of the contract whichever is earlier or as intimated in the work order issued by MMRC |
| 5. | Performance Security Deposit (BG) validity period | Performance Security Deposit should be valid for 6 months from the end of contract |

| | | |
|---|---|---|
| 6. | Last date for signing contract | As intimated in work order of MMRC |
| 7. | Contract Period | 5 Years post Go-Live |

*Note: Prospective Bidders may visit MMRC IT Office for any further information/clarification regarding this RFP on prior appointment during working hours till the date of technical bid submission.*

# 3. Instructions to Bidders

## 3.1 Introduction of MMRC

Mumbai Metro Rail Corporation Limited (MMRC) is a Joint Venture (50:50) Company of Government of India and Government of Maharashtra. MMRC is responsible for the implementation of Mumbai Metro Rail Line-3.

MMRC has envisioned the development of an integrated IT enabled e-governance system across the organization in order to ensure transparent, easy, efficient and accurate availability of information, and facilitation of transactions. With intent of providing a robust system, MMRC has decided to structure its current systems and core functions through e-governance solutions by leveraging Information and Communication Technology across various functions in the organization.

MMRC has enterprise systems like ERP and eOffice which it plans to host on a Cloud Model for Disaster Recovery.

## 3.2 Purpose

MMRC seeks the services of from reputed, competent and professional Information Technology (IT) companies, who meet the Pre-Qualification Criteria as specified in this bidding document for the "**RFP for Hiring of "Cloud based Disaster Recovery services" from Managed Service Provider at Mumbai Metro Rail Corporation (MMRC)**". This document provides information to enable the bidders to understand the broad requirements to submit their bids. The detailed scope of work is provided in Section 4 of this RFP document.

**Address for Correspondence & Contact Person:**

Shri. R. K Sharma,
Executive Director (Electrical),
5th Floor, MMRDA Old Building,
Bandra Kurla Complex,
Bandra (East)
Mumbai—400 051

E-mail: itpmo.mmrc@gmail.com

## 3.3 Consortium

The consortium or joint ventures are not allowed.

## 3.4 Sub-Contracting Conditions

1. The Bidder can sub-contract project activities only related to installation, commissioning configuring and maintenance of Connectivity from Cloud Service Provider to MMRC. However, it is clarified that the Bidder shall be the principal employer for all claims

arising from the liabilities statutory or otherwise, concerning the sub-contractors. The Bidder undertakes to indemnify the Nodal Agency or its nominated agencies from any claims on the grounds stated hereinabove.

2. The bidder shall share all the details of the Service Provider in the Technical Bid. Both during the process of award, and post award of contract, if there is a change in sub-contractor, the Bidder shall obtain prior permission form MMRC.

## 3.5 Completeness of Response

1. Bidders are advised to study all instructions, forms, terms, requirements and other information in the RFP documents carefully. Submission of bid shall be deemed to have been done after careful study and examination of the RFP document with full understanding of its implications.
2. The response to this RFP should be full and complete in all respects. Failure to furnish all information required by the RFP document or submission of a proposal not substantially responsive to the RFP document in every respect will be at the Bidder's risk and may result in rejection of its Proposal.

## 3.6 Proposal Preparation Costs

1. The bidder shall submit the bid at its cost and MMRC shall not be held responsible for any cost incurred by the bidder. Submission of a bid does not entitle the bidder to claim any cost and rights over MMRC and MMRC shall be at liberty to cancel any or all bids without giving any notice.
2. All materials submitted by the bidder shall be the absolute property of MMRC and no copyright/patent etc. shall be entertained by MMRC.

## 3.7 Bidder Inquiries

Bidder shall e-mail their queries at above mentioned e-mail address, in the format as prescribed in the section 6.3. The response to the queries will be published on www.tenderwizard.com/MMRC. No queries will be entertained thereafter. This response of MMRC shall become integral part of RFP document. MMRC shall not make any warranty as to the accuracy and completeness of responses.

## 3.8 Amendment of RFP Document

1. All the amendments made in the document would be published on the e-Tendering Portal and shall be part of RFP.
2. The Bidders are advised to visit the aforementioned website/portal on regular basis to check for necessary updates. The MMRC also reserves the right to amend the dates mentioned in this RFP.

## 3.9 Supplementary Information to the RFP

If MMRC deems it appropriate to revise any part of this RFP or to issue additional data to clarify an interpretation of provisions of this RFP, it may issue supplements to this RFP. Any such corrigendum shall be deemed to be incorporated by this reference into this RFP.

## 3.10 MMRC's right to terminate the process

MMRC may terminate the RFP process at any time and without assigning any reason. MMRC reserves the right to amend/edit/add/delete any clause of this Bid Document. This will be informed to all and will become part of the bid/RFP and information for the same would be published on the e-Tendering portal.

## 3.11 Earnest Money Deposit (EMD)

1. Bidders shall submit, EMD of Rs. 2, 20, 000/- (Rupees Two Lakhs Twenty Thousand Only) through Online e-Tendering Payment Gateway mode only.
2. Unsuccessful bidder's EMD will be returned within 90 days from the date of opening of the financial bid. The EMD for the amount mentioned above, of the successful bidder would be returned upon submission of Performance Security Deposit (Bank Guarantee) for an amount equal to 10% of Total Contract Value in the format provided in Annexure B of the RFP.
3. No interest will be paid by MMRC on the EMD amount and EMD will be refunded to the all Bidders (including the successful Bidder) without any accrued interest on it.
4. The Bid submitted without EMD, mentioned above, will be summarily rejected
5. The EMD may be forfeited:
   a) If a Bidder withdraws his bid or increases his quoted prices during the period of bid validity or its extended period, if any.
   b) In case of a successful bidder, if the Bidder fails to sign the contract in accordance with the terms and conditions.
   c) If during the bid process, a bidder indulges in any such deliberate act as would jeopardise or unnecessarily delay the process of bid evaluation and finalisation.
   d) If, during the bid process, any information is found false/fraudulent/mala fide, and then MMRC shall reject the bid and, if necessary, initiate action.

## 3.12 Authentication of Bid

1. The original copy (hard copy) of the Bid Document shall be signed, stamped and submitted along with the bid. Authorized person of the bidder who signs the bid shall obtain the authority letter from the bidder, which shall be submitted with the Bid. All pages of the bid and its annexures, etc. shall be signed and stamped by the person or persons signing the bid.
2. Registered/ irrevocable Power of Attorney executed by the Bidder in favour of the duly authorised representative, certifying him as an authorised signatory for the purpose of

this bid. In the case of the Board resolution authorizing a person as the person responsible for the bid, the Board resolution shall be submitted. The person accountable for the bid shall remain the full time employee of the bidder till the end of contract period.

## 3.13 Language of Bids

This bid should be submitted in English language only. If any supporting documents submitted are in any language other than English, then the translation of the same in English language is to be duly attested by the bidder and summited with the bid, and English translation shall be validated at MMRC's discretion.

## 3.14 Patent Claim

In the event of any claim asserted by a third party of infringement of copyright, patent, trademark or industrial design rights arising from the use of the goods or any part thereof, the bidder shall expeditiously extinguish such claim. If the bidder fails to comply and MMRC is required to pay compensation to a third party resulting from such Infringement, the Bidder shall be responsible for such compensation, including all expenses, court costs, lawyer fees etc. MMRC shall give notice to the Successful Bidder(s) of any such claim and recover it from the bidder.

## 3.15 Bid Submission Format

The entire proposal shall be submitted strictly as per the format specified in this Request for Proposal. Bids with deviation from this format are liable for rejection.

## 3.16 Bid Submission Instructions

Complete bidding process will be online (e-Tendering) in two envelope system. Submission of bids shall be in accordance to the instructions given in the Table below:

| Particulars | Instructions |
|---|---|
| **Envelope A:**<br>**Technical Proposal** | Scanned copy of Receipt of the Tender Fees and Earnest Money Deposit (EMD) must be uploaded through online bid submission process.<br>The Pre-qualification documents and Technical documents shall be prepared in accordance with the requirements specified in this RFP and the formats are prescribed in in Section 6 of this RFP. Bidders shall submit accurately filled Checklist for Pre-qualification documents and Technical evaluation documents as per format in section 6.7 and section 6.8.<br>Each page of the Technical Proposal should be signed and stamped by the Authorized Signatory of the Bidder. Technical Proposal should be submitted through online bid submission process only. |

| Particulars | Instructions |
|---|---|
| **Envelope B: Financial Proposal** | The Financial Proposal shall be prepared in accordance with the requirements specified in this RFP and in the formats prescribed in Section 7 of the RFP.<br>Each page of the Financial Proposal should be signed and stamped by the Authorized Signatory of the Bidder. Financial Proposal should be submitted through online bid submission process only. |

The following points shall be kept in mind for submission of bids;

1. MMRC shall not accept delivery of proposal in any manner other than that specified in this RFP. Proposal delivered in any other manner shall be treated as defective, invalid and rejected.
2. The Bidder is expected to price all the items and services sought in the RFP and proposed in the proposal. The Bid should be comprehensive and inclusive of all the services to be provided by the Bidder as per the scope of his work and must cover the entire Contract Period.
3. MMRC may seek clarifications from the Bidder on the Technical proposal. Any of the clarifications by the Bidder on the Technical proposal should not have any commercial implications. The Financial Proposal submitted by the Bidder should be inclusive of all the items in the Pre-Qualification proposal and should incorporate all the clarifications provided by the Bidder on the Pre-Qualification proposal during the evaluation of the Pre-Qualification offer.
4. Financial Proposal shall not contain any technical information.
5. If any Bidder does not qualify the prequalification criteria stated Section 3.23 of this RFP and doesn't meet minimum qualifying marks for technical evaluation, the financial proposals of the Bidder shall not be opened in the e-Tendering system.
6. It is required that the all the proposals submitted in response to this RFP should be unconditional in all respects, failing which MMRC reserves the right to reject the proposal.
7. Proposals sent by fax/post/courier shall be rejected.

## 3.17 Late Proposal and Proposal Validity Period

Proposals received after the due date and the specified time (including the extended period if any) for any reason whatsoever, shall not be entertained and shall not be opened in the e-Tendering system. The validity of the proposals submitted before deadline shall be till 180 days from the date of submission of the proposal.

## 3.18 Modification and Withdrawal of Proposals

No Proposal shall be withdrawn in the interval between the deadline for submission of proposals and the expiration of the validity period specified by the Bidder on the Proposal form. Entire EMD shall be forfeited if any of the Bidders withdraw their proposal during the validity period.

## 3.19 Non-conforming Proposals

A Proposal may be construed as a non-conforming proposal and ineligible for consideration:

1. If it does not comply with the requirements of this RFP.
2. If the Proposal does not follow the format requested in this RFP or does not appear to address the particular requirements of the MMRC.

## 3.20 Acknowledgement of Understanding of Terms

By submitting a Proposal, each Bidder shall be deemed to acknowledge that he/she has carefully read all sections of this RFP, including all forms, schedules, annexure, corrigendum and addendums (if any) hereto, and has fully informed itself as to all existing conditions and limitations.

## 3.21 Bid Opening

1. Total transparency shall be observed and ensured while opening the Proposals/Bids
2. MMRC reserves the rights at all times to postpone or cancel a scheduled Bid opening.
3. Bid opening shall be conducted in two stages.
4. In the first stage, Technical Envelope of proposals shall be opened and evaluated as per the pre-qualification and technical evaluation criteria mentioned in Section 3.23 of the RFP and Section 3.25 of the RFP.
5. In the second stage, Commercial Proposals of those Bidders, who qualify Pre-Qualification Criteria and Technical criteria, shall be opened. All Bids shall be opened in the presence of Bidders' representatives who choose to attend the Bid opening sessions on the specified date, time and address.
6. The Bidders' representatives who are present shall sign a register evidencing their attendance. In the event of the specified date of Bid opening being declared a holiday for MMRC, the bids shall be opened at the same time and location on the next working day. In addition to that, if there representative of the Bidder remains absent, MMRC will continue process and open the bids of the all bidders.
7. During Bid opening, preliminary scrutiny of the Bid documents shall be made to determine whether they are complete, whether required Bid Security has been furnished, whether the Documents have been properly signed, and whether the bids are generally in order. Bids not conforming to such preliminary requirements shall be prima facie rejected. MMRC has the right to reject the bid after due diligence is done.

## 3.22 Evaluation Process

1. MMRC shall evaluate the Tender Fee, EMD, Pre-Qualification documents and Technical Evaluation documents (Envelope A), and Financial Proposal (Envelope B) and submit its

recommendation to the Competent Authority whose decision shall be final and binding upon the bidders.

2. Bidders shall be evaluated as per the pre-qualification and technical evaluation criteria mentioned in Section 3.23 of the RFP and Section 3.25 of the RFP.
3. Bidders with minimum technical score of 60 out of 100 in technical evaluation (Refer Section 3.25) will be considered to be eligible for financial evaluation (Refer Section 3.27)
4. Amongst the bidders who are considered for financial evaluation, the bidder who has quoted the Least will be considered as most eligible for award, at the discretion of MMRC. MMRC, however reserves the right to accept or reject any or all bids without giving any reasons thereof.
5. The bidder shall provide required supporting documents with respect to the Pre-Qualification Proposal, Technical Proposal evaluation as per the criteria mentioned in Section 3.23 and Section 3.25 of this RFP.
6. Please note that MMRC may seek inputs from their professional, external experts in the Bid evaluation process.
7. In no way the bidder shall indicate its Financial Offer in any Envelope other than Envelope B. In case it is found, MMRC may summarily reject the proposal of the said bidder.

## 3.23 Prequalification criteria

### A. For Managed Service Provider (MSP)

| Sr. No. | Basic Requirement | Eligibility Criteria | Documents to be submitted |
|---|---|---|---|
| PQ1 | Legal Entity | The MSP should be a company registered under the Companies Act, 2013 or the Companies Act, 1956 OR a Limited Liability Partnership (LLP) registered under the LLP Act, 2008 or Indian Partnership Act 1932 | Copy of Certificate of Incorporation/ Registration/Partnership deed<br>Copy of PAN Card<br>Copy of GST Registration |
| PQ2 | Turnover | The MSP should have minimum average annual turnover of Rs. 3.5 crore from Data Centre business in India for the last three financial years (FY 14-15, FY 15-16, FY 16-17) | Certificate from the Statutory Auditor / Chartered Accountant clearly stating the Turnover from Data Centre business or Annual Report stating Turnover from Data Centre business |

| | | | |
|---|---|---|---|
| PQ3 | Capability | The MSP should have successfully implemented/commissioned at least 1 (one) project of DC/DR with Cloud deployment with an order value of minimum Rs. 1.76 Cr hosted out of the proposed DC / DR facility in India.<br>OR<br>at least 2 (two) projects of DC/DR with Cloud deployment with an order value of minimum Rs, 1.32 Cr hosted out of the proposed DC / DR facility in India.<br>OR<br>at least 3 (three) projects of DC/DR with Cloud deployment with an order value of minimum Rs. 88 Lakhs hosted out of the proposed DC / DR facility in India<br>Note:<br>In case of an ongoing project, the percentage of work completed for must be at least 50%. | Work order + Completion Certificates from the client;<br>OR<br>Work Order + Self Certificate of Completion (Certified by the Statutory Auditor);<br>OR<br>Work Order + Phase Completion Certificate by client |
| PQ4 | Blacklisting | The Bidder should not be debarred/ blacklisted by any Government/PSU in India as on date of submission of the Bid. | A self-certified letter signed by the Authorized Signatory of the Bidder as per Annexure A. |

## B. For Cloud Service Provider (CSP)

| Sr. No. | Basic Requirement | Eligibility Criteria | Documents to be submitted |
|---|---|---|---|
| PQ1 | Legal Entity | The CSP should be a company registered under the Companies Act, 2013 or the Companies Act, 1956 OR a Limited Liability Partnership (LLP) | Copy of Certificate of Incorporation/ Registration/Partnership deed |

| | | | |
|---|---|---|---|
| | | registered under the LLP Act, 2008 or Indian Partnership Act 1932. | Copy of PAN Card<br>Copy of GST Registration |
| PQ 2 | Data Center Facility | The Data Center facility must meet all of the following criteria: | |
| PQ 2(1) | | Should confirm to Tier III standards/ and the certificate/rating should be valid at the time of bidding. | Valid Copy of the Tier III Certification, certified under TIA 942 or Uptime Institute certifications by a 3rd party |
| PQ 2(2) | | Data Center and Disaster Recovery Center Facilities must be certified for ISO 27001 / 27018 (year 2013 or above) and provide service assurance and effectiveness of Management compliant with ISO 20000 standards. | Valid Copy of the ISO 27001 / 27018, ISO 20000 Certification |
| PQ 3 | Products /OEM Solution offered | The OEM whose Cloud / Virtualization Solution are being proposed should have at least 10 implementations of the same product in third party Data Centers in India.<br>The Bidder must be authorized by OEM (Original Equipment Manufacturer) in India for Cloud Solution / Virtualization Solution offering. | OEM certification for usage in at least 10 implementations in third party Data Centers in India.<br>Manufacturer's authorization Form from OEM |
| PQ 4 | MeitY Empanelment | The Cloud Service Provider shall be empaneled and audit compliant as per Ministry of Electronics and Information Technology (MeitY). | Letter of Empanelment / Certificate of Empanelment from MeitY (Empanelment should be current and applicable as on bid submission date) |
| PQ 5 | Proposed DR Site | Proposed DR site should be in a different Seismic Zone than the current MMRC DC at Bandra Kurla Complex, Mumbai. | Letter from authorized signatory on the letter head of CSP mentioning the address of the proposed MeitY / Cert-in Certified Disaster Recovery Site |

| | | | |
|---|---|---|---|
| PQ 6 | Blacklisting | The Bidder should not be debarred/ blacklisted by any Government/PSU in India as on date of submission of the Bid. | A self-certified letter signed by the Authorized Signatory of the Bidder as per Annexure A. |

Note:

- Managed Service Provider and Cloud Service Provider may be single entity, in such cases will need qualify for conditions of Managed Service Provider and Cloud Service Provider.
- Managed Service Provider shall be solely liable to and responsible for all obligations towards the performance of works/services including that of its partners/associates under the contract.

## 3.24 Evaluation of Prequalification Proposals

1. Bidders, whose EMD and RFP Document Fees are found in order, shall be considered for Pre-Qualification criteria evaluation.
2. Bidder shall be evaluated as per prequalification criteria mentioned at Section 3.23. The bidders who fulfil all the prequalification criteria and technical demo shall qualify for further commercial evaluation.
3. The Bidders are required to submit all required documentation in support of the evaluation criteria specified (e.g. Detailed Project citations and completion certificates, client contact information for verification, and all others) as required for pre-qualification evaluation.
4. At any time during the Bid evaluation process, MMRC may seek oral / written clarifications from the Bidders. MMRC may seek inputs from their professional and technical experts in the evaluation process.
5. MMRC reserves the right to do a reference check of the past experience stated by the Bidder. Any feedback received during the reference check shall be taken into account during the pre-qualification evaluation process.

## 3.25 Technical Evaluation Criteria

| # | Criteria | Evaluation parameters | Maximum Marks | Documents Required |
|---|---|---|---|---|
| TQ 1 | Experience of Bidder in offering cloud services (IaaS) in India or Globally | 2-5 years : 6 marks<br>6-9 years : 8 marks<br>10+ years : 10 marks | 10 | Project Work order / Completion Certificates from the client stating Project Start date and Project End date |

| | | | | |
|---|---|---|---|---|
| TQ 2 | Tier Classification of the proposed Data Center, where cloud hosting is to be served from : | Tier III : 3 marks<br>Tier IV : 5 marks | 5 | Valid Copy of the Tier III or Tier V Certification, certified under TIA 942 or Uptime Institute certifications by a 3rd party |
| TQ 3 | Data Centre Uptime in Last 4 quarters | <99.5% : 0 marks<br>99.5-99.9% : 5 marks<br>>99.9% : 10 marks | 10 | Self-undertaking along with system generated report |
| TQ 4 | Number of VMs running (active) in the DC of the bidder | 200-400 VM's : 6 marks<br>401-600 VM's : 8 marks<br>>=601 VM's : 10 marks | 10 | Self-undertaking along with report showing number of VM's running from proposed DC/DR facility |
| TQ 5 | Compliance to functional requirements | If compliance<br>>95% - 15 marks<br>85-95% - 10 marks<br>70-85% 5 marks | 15 | Compliance sheet as per section 4.11.2 to be submitted, signed and stamped by Authorized Signatory |
| TQ 6 | Project Manager Exp. in terms of Data Center Management, Cloud Solution Design and Management | 8-11 years : 6 marks<br>12-15 years: 8 marks<br>>=16 years : 10 marks | 10 | CV for Proposed Resource |
| TQ 7 | MSP's experience in setting up IT Infra on cloud based DC/DR for minimum order value of Rs. 88 Lakhs hosted out of the proposed DC / DR facility in India | 1 project : 3 marks<br>Every additional project: 3 marks, max. upto 15 marks | 15 | Project Work order and Completion Certificates |

| | | | | |
|---|---|---|---|---|
| TQ 8 | Technical Presentation | Bidders understanding of the project and Scope of Work – 5 marks | 25 | |
| | | Technical Solution – 5 marks | | |
| | | Project Management Methodology and People / Resources – 5 marks | | |
| | | Demonstration of the cloud solution – 5 marks | | |
| | | Clarifications / Answers given to the Bid Evaluation Committee during the Presentation – 5 marks | | |
| | | Total | 100 | |

## 3.26 Technical Evaluation Methodology

1. The Financial Proposals of Bidders who do not qualify technically shall be kept unopened in the e-Tendering system.
2. MMRC reserve the right to accept or reject any or all bids without giving any reasons thereof.
3. MMRC shall inform to the technically shortlisted Bidders about the date and venue of the opening of the financial proposals.

## 3.27 Commercial Evaluation

1. Of all the financial proposal opened, the Bidder whose financial proposal is lowest (hereby referred to as L1 Bidder) shall be considered as most eligible for award of contract.
2. If there is a discrepancy between words and figures, the amount in words shall prevail. For any other calculation/ summation error etc. the bid may be rejected.

## 3.28 Award of Contract

### 3.28.1 MMRC's Right to accept any Bid and to reject any or All Bids

MMRC reserves the right to accept or reject any Bid, and to annul the bidding process and reject any or all Bids at any time prior to award of Contract, without thereby incurring any liability to the affected Bidder or Bidders or any obligation to inform the affected Bidder or Bidders of the grounds for MMRC's action.

### 3.28.2 Letter of Acceptance

Prior to the expiration of the period of bid validity, MMRC will notify the successful bidder in writing or by fax or email, to be confirmed in writing by letter, that its bid has been accepted. The Letter of Acceptance will constitute the formation of the contract. Upon the Successful Bidder's furnishing of Performance Security Deposit, MMRC will promptly notify each unsuccessful Bidder.

### 3.28.3 Signing of Contract

MMRC shall notify the successful bidder that its bid has been accepted. The Successful Bidder shall enter into contract agreement with MMRC within the time frame mentioned in the Letter of acceptance to be issued to the successful bidder by MMRC.

### 3.28.4 Failure to agree with the Terms & Conditions of the RFP / Contract

Failure of the successful Bidder to agree with the Terms & Conditions of the RFP / Contract shall constitute sufficient grounds for the annulment of the award, in which event MMRC may invite the next best bidder for negotiations or may call for fresh RFP.

## 3.29 Award Criteria

1. The bidder who has quoted the least will be adjudicated as most eligible for award of the Project.
2. However, MMRC reserves the right to further negotiate the prices quoted by the most responsive bidder.

## 3.30 Non-Disclosure Agreement (NDA)

The Successful Bidder(s) has to sign the Non- Disclosure Agreement (Annexure C) with MMRC.

## 3.31 Instructions for Proposed Resource

1. The Bidder is required to provide the CVs for each of the positions specified. Only 1 CV must be provided for each profile mentioned. In case more than 1 CV is provided, the first one provided for the profile shall be used for the purpose of evaluation.
2. In case no CVs are proposed for any of the specified positions, the technical score would be adjusted proportionately. Though resource persons suggested for additional posts would be considered during evaluation, not proposing additional posts would not detract from the qualification of a Bidder.
3. CVs of all resource persons proposed MUST be furnished in the format given at Section 6.5.1 (Max 3 pages per CV). Non-adherence to the format or missing information in the specified format would amount to rejection of the CV for evaluation, at the discretion of the MMRC Tender Evaluation Committee.
4. Only the relevant Projects of each resource person may be detailed in the CV.
5. Each profile shall be signed by the resource (of whom the profile is submitted) and the authorized Signatory of the Bidder. If the signature of the resource cannot be obtained, the Authorized Signatory, in each profile shall mention and certify that he has obtained the consent of the respective employee on the accuracy and completeness of qualifications, experience and other details specified in the profile.
6. The Tender Evaluation Committee may, at its discretion, request the Bidder to provide additional details with respect to any or all of the personnel proposed, if required in the evaluation process.
7. The Successful Bidder shall confirm the availability of the team members as proposed in the Technical proposal. MMRC will not consider changes or substitutions during negotiations as the ranking of the Bidder is based on the evaluation of the proposed profiles, and any change therein may upset the ranking. Changes or substitutions, will, however be permitted if the proposed man power is not available for reasons of any incapacity due to health.
8. In case, replacement is required, the Selected Bidder shall notify MMRC in writing at least 15 (Fifteen) days in advance, for prior approval, stating: the reason for replacing the person(s), originally assigned to the project the names and signed curriculum vitae (CV) of the proposed replacement. MMRC may also request replacement with valid reason.
9. Changes or Substitutions of the Project Manager shall not be considered and may lead to disqualification of the Bidder or termination of the contract.

## 3.32 Security Deposit

1. The successful bidder needs to deposit/submit a security deposit equal to 10% of total contract value as Bank Guarantee from nationalised bank only. The security deposit shall be valid for a period of 6 months from the end of contract. It should be submitted within fourteen (14) working days of the date of notice of award of the contract or prior to signing of the contract whichever is earlier or as intimated in the work order issued by

MMRC due and proper fulfilment of bid document conditions. Total contract value shall be calculated based on an estimated number of cards to be issued and rate finalized as per financial format in this tendering process.

2. The security deposit should be submitted within the period specified above, failing which MMRC may cancel the offer made to the bidder.
3. The security deposit will be forfeited if vendor has not fulfilled the terms and conditions as per bid document.
4. MMRC shall also be entitled to make any recoveries due from the bidder from security deposit submitted against this bid document. In such case the bidder will have to recoup the security deposit amount so recovered within 10 days.
5. The security deposit shall be retained by MMRC for the period of 6 months from the end of contract. No interest will be payable by the MMRC on the amount of the Bid Security.
6. Security Deposit will be released after 6 months from the end of contract or completion of all work whichever is later.

## 3.33 Bid Prices

The vendor has to quote for "**Hiring of "Cloud based Disaster Recovery Services" from Managed Service Provider at Mumbai Metro Rail Corporation (MMRC)"**, in the format given for financial bid. Validity of Bid shall be of 180 days from date of opening of bids.

## 3.34 Bid Currency

The rates quoted shall be in Indian Rupees only.

## 3.35 Signature

A representative of the bidder, who is authorized to commit the bidder to contractual obligations, must sign with the bidder's name and seal on all pages of the Bid, including the tender/bid document. All obligations committed by such signatories must be fulfilled.

## 3.36 Correction of errors

The vendor is advised to take adequate care in quoting the rate. No excuse for corrections in the quoted rate will be entertained afterwards. The corrections or overwriting in bid document should be initialed by person signing the Bid form.

## 3.37 Corrections to Arithmetic errors

In case of discrepancy between the amounts mentioned in figures and in words, the amount in words shall govern. The amount stated in the Bid form, adjusted in accordance with the above procedure, shall be considered as binding.

## 3.38 Disqualification

The Bid from the bidders is liable to be disqualified in the following cases:

1. Bid not submitted in accordance with the bid document.
2. The bidder qualifies the bid with his own conditions.
3. During validity of the Bid, or its extended period, if any, the bidder increases his quoted prices.
4. Bid is received in incomplete form.
5. Bid is received after due date and time.
6. Bid is not accompanied by all requisite supporting documents.
7. Information submitted in Pre-Qualification Bid is found to be misrepresented, incorrect or false, accidentally, unwittingly or otherwise, at any time during the processing of the contract (no matter at what stage) or during the tenure of the contract including the extension period if any.
8. The successful bidder fails to enter into a contract within 10 working days of the date of notice of award of contract or within such extended period, as fixed by MMRC.
9. Awardee of the contract has given the letter of acceptance of the contract with his conditions.
10. Non-fulfilling of any condition/term by bidder.

# 4. Scope of Work

MMRC wishes to engage a Managed Service Provider to provide Cloud based Disaster Recovery services for a period of 5 years post Go-Live for this project.

Scope of Work Overview

| Sr. No | Particulars | Description |
|---|---|---|
| 1. | Managed Cloud Service for Disaster Recovery | • Design, configuration, installation and setup of Disaster Recovery at Cloud. DR Database Storage shall be replicated on an ongoing basis and shall be available in full (100% of the DC) as per designed RTO/RPO.<br>• Maintenance & Support of Cloud solution.<br>• Change Management Workshops. |
| 2. | Connectivity from Cloud Service Provider to MMRC | Installation, configuration, maintenance and upkeep of 10 Mbps point to point Leased Line Connectivity from Cloud Service Provider to MMRC, inclusive of labor cost, consumables cost, civil work like digging, trenching, etc. and coordination with required authorities. Link shall be terminated at both MMRC building (at distance of 300-500 meters) to ensure internet connectivity at all times. MMRC may move its office to a new building (at distance of 100 meters) in future, service provider shall support, install and commission internet link. |
| 3. | Configuration of Data center Site at MMRC premises | Configuration and Monitoring of Data Center Site at MMRC Premises. |

## 4.1 General Requirements

- Service Provider should ensure that the data should be residing within India. Data should only be accessed by entities authorized by MMRC.
- MMRC shall retain ownership of any user created/loaded data and applications hosted on Service Provider's infrastructure and maintains the right to request (or should be able to retrieve) full copies of these at any time.

- MMRC retains ownership of all virtual machines, templates, clones, and scripts/applications created for the MMRC's application. MMRC retains the right to request (or should be able to retrieve) full copies of these virtual machines at any time.
- Service Provider should be accessible via internet and P2P links
- Service Provider should offer support 24 hours a day, 7 days a week, 365 days per year via its Network Operation Centre for monitoring and management of proposed IT infrastructure / Cloud services.
- Service Provider should manage provisioned infrastructure as per the ITIL standards
- Service Provider's shall provide interoperability support with regards to available APIs, data portability etc., for the Government Department to utilize in case of Change of cloud service provider, migration back to in-house infrastructure, burst to a different cloud service provider for a short duration or availing backup or DR services from a different service provider.
- Shall adhere to the ever evolving guidelines as specified by CERT-In (http://www.cert-in.org.in/)
- Shall adhere to the standards published (or to be published) by MeitY or any standards body setup / recognized by Government of India and notified to the Service Provider by MeitY as a mandatory standard.
- The Service Provider's cloud service offerings will have to comply with the guidelines & standards as and when such guidelines / standards are published by MeitY within the timeframe given by MeitY. Service Provider is responsible for all costs associated with implementing, assessing, documenting and maintaining the empanelment.
- Service Provider should offer monitoring tools that should monitor resources such as compute and other resources to gain system-wide visibility into resource utilization and operational health. MMRC should get the appropriate visibility for the monitored information via a web dashboard.
- It is expected that compute, storage, and bandwidth requirements may be auto-scaled (additional capacity based on the demand and auto-scaling rules) over the period of the contract in line with the transaction load to meet the SLA requirements. The application must be architected and designed to leverage the cloud characteristics such as rapid elasticity and handle transient and hardware failures without downtime.
- The Service Provider will be responsible for adequately sizing the necessary compute, memory, and storage required, building the redundancy into the architecture (including storage) and load balancing to meet the service levels mentioned in the RFP.
- It is expected that the Service Provider, based on the growth in the user load (peak and non-peak periods; year-on-year increase), will scale up or scale down the compute, memory, storage, and bandwidth requirements to support the scalability and performance requirements of the solution and meet the SLAs.

## 4.2 Infrastructure Analysis and Build

Under this phase Vendor needs to examine existing IT infrastructure and administrative functionality and applications at the primary data center of MMRC (the "As Is" architecture) to make their Plan. During this phase a standard operating environment is created as a baseline "To Be" architecture.

**Details of Existing Infrastructure:**

**A. ERP**

| Sr. No | Make & Model | CPU | RAM | HDD | OS | Role |
|---|---|---|---|---|---|---|
| 1. | DL360 Gen9 | 2 x 8 Cores | 128GB | 2 x 600GB | Oracle VM Host 3.3.1 | Oracle VM Host |
| 2. | DL360 Gen9 | 2 x 8 Cores | 128GB | 2 x 600GB | Oracle VM Host 3.3.1 | Oracle VM Host |
| 3. | DL360 Gen9 | 2 x 8 Cores | 128GB | 2 x 600GB | Oracle VM Host 3.3.1 | Oracle VM Host |
| 4. | DL360 Gen9 | 2 x 8 Cores | 128GB | 2 x 600GB | VOMM: 3.4.2.1384 | OVMM + Backup Server |
| 5. | HP MSA 2040 | Disk Details : 600GB x 13 SAS 10K 2.5in HDD | | | | SAN Storage |

| Sr. No | Host Name (VMs) | CPU | RAM | HDD | OS |
|---|---|---|---|---|---|
| 1. | MMRCLPRODAPPDB | 6 | 64GB | 1.4TB | Oracle Ent. Linux 6.6 |
| 2. | MMRCLUATAPPDB | 4 | 48GB | 1.2TB | Oracle Ent. Linux 6.6 |
| 3. | MMRCLHPDPCON | 4 | 8GB | 100GB | Windows 7 |

Number of Users for ERP is around 250.

**Data Usage Details**

| Sr. No | Particulars | |
|---|---|---|
| 1. | Approximate Initial Data | 350 GB |
| 2. | Approximate Per day Average Data | 284 MB |

Note: Above data usage is only approximate figure. Data usage is bound to change depending on user's requirement like uploading of documents, heavy files etc.

**Software and Licensing Details**

| Sr. No | Description of Oracle Programs | Metric | Term | Quantity Purchase |
|---|---|---|---|---|
| 1. | Oracle Financials – Application User Perpetual | Application User | Perpetual | 25 |

| | | | | |
|---|---|---|---|---|
| 2. | Oracle Internet Expenses – Expenses Reports Perpetual | Expenses Reports | Perpetual | 200 |
| 3. | Oracle Purchasing – Application User Perpetual | Application User | Perpetual | 10 |
| 4. | Oracle Discrete Manufacturing - Application User Perpetual | Application User | Perpetual | 10 |
| 5. | Oracle Human Resources – Employee Perpetual | Employee | Perpetual | 200 |
| 6. | Oracle Self Service Human Resources - | Employee | Perpetual | 200 |
| 7. | Oracle Payroll – Employee Perpetual | Employee | Perpetual | 200 |
| 8. | Oracle iRecruitment Information Discovery – Employee Perpetual | Employee | Perpetual | 200 |
| 9. | Oracle Learning Management – Trainee Perpetual | Trainee | Perpetual | 200 |
| 10. | Oracle Database Enterprise Edition – Name User Plus | Named User Plus | Perpetual | 50 |
| 11. | Oracle Internet Developer Suite – Named User Plus | Named User Plus | Perpetual | 1 |
| 12. | Oracle Weblogic Suite – Named User Plus Perpetual | Named User Plus | Perpetual | 30 |
| 13. | Oracle Virtual Machine | | | 1 |
| 14. | Oracle Enterprise Linux | | | 1 |

**B. e-Office**

| Sr. No. | Application Name | Core | RAM(GB) | HDD | Operating System | DB / APP | Server Type |
|---|---|---|---|---|---|---|---|
| 1. | App Server - VM1 | 8 | 64 | 1 TB | RHEL 7.2 64 Bit | APP | Virtual |
| 2. | DB Server - VM2 | 6 | 64 | 500 GB | RHEL 7.2 64 Bit | DB | Virtual |
| 3. | Streaming - Replication Server | 6 | 64 | 500 GB | RHEL 7.0 64 Bit | APP | Virtual |
| 4. | DB Backup Server | 2 | 32 | 500 GB | RHEL 7.0 64 Bit | APP | Virtual |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| 5. | Demo APP + DB Server | 4 | 32 | 500 GB | RHEL 7.2 64 Bit | APP+DB | Virtual |
| 6. | CRL Server | 4 | 32 | 500 GB | RHEL 7.2 64 Bit | | |
| 7. | Local DNS Sever - win server 2008 | 2 | 16 | | Win2k8 64 Bit | | Virtual |
| 8. | SAN Storage | | | 2 TB | | | Storage |

Number of Users for e-Office is around 250.

**Data Usage Details**

| Sr. No | Particulars | |
|---|---|---|
| 1. | Approximate Initial Data | 213 GB |
| 2. | Approximate Per day Average Data | 1.2 GB |

Note: Above data usage is only approximate figure. Data usage is bound to change depending on user’s requirement like uploading of documents, heavy files etc.

**Licensing Details**

| Sr. No | Particulars |
|---|---|
| 1. | VMware vSphere 6 Enterprise Licensed for 2 physical CPUs (unlimited cores per CPU) |
| 2. | RHEL 7.2 64 Bit |
| 3. | Windows Server 2008 R2 Enterprise Edition 64 Bit |

The current infrastructure mentioned above is provided for overall understanding of requirement at MMRC. Bidder may visit MMRC departments (On prior approval of MMRC and its officials) and understand these requirements in detail.

The first step in this process is to identify the existing infrastructure applications. These applications include services that perform a business role and are required for proper functionality in DR environment. The analysis is conducted by working very closely with MMRC’s IT staff — reviewing installation methods, network topology, authentication procedures, and any existing documentation for third-party software. The bidder is expected to capture the current infrastructure details and MMRC's requirements and propose optimal solution meeting MMRC's requirement.

### 4.2.1 Infrastructure ecosystem mapping

Vendor should map MMRC existing infrastructure applications to their Solution.

### 4.2.2 Operating System Build:

Bidder needs to study the existing infrastructure including operating system and provisioning of operating system at Cloud site should be planned accordingly.
Provisioning is composed of the following components:

- Provisioning configuration
  - Installation methodologies
  - Software packages
  - Configurations according to security, authentication, storage, and other requirements
- Testing
  - Provisioning server setup
  - Deployment testing
  - Adherence to policy and configuration
- Delivery and training
  - Customer's IT staff trained to deploy and modify SOE build
  - Any remaining customer needs addressed
  - Additional training recommendations
- Documenting Results
  - Documentation
  - Detailing work performed
  - Specific procedures
  - Recommendations for future enhancements or growth
  - Links to product-specific manuals
- Fully tested provisioning server and provisioning configuration file(s)
- Time-tested and precise methodology, freeing up resources

## 4.3 Functional Application Analysis

### 4.3.1 Application Information Gathering

Vendor should examine existing documentation and conducting interviews with various IT and business stakeholders and should include below data in it:

- Existing hardware characteristics for different environments like production, staging, testing, and development environments
  - Number of hosts / CPUs per host
  - Memory requirements
  - Storage and file system requirements
  - Network bandwidth and latency requirements
  - Horizontal scalability requirements and/or limitations
  - Vertical scalability requirements and/or limitations
  - Hardware utilization rates

- Security requirements
- Authentication and authorization
- Versions and ISV support levels
- Specific software dependencies
- Development languages and platforms
- External integration points
- Virtualization restrictions
- Performance
- Stability

### 4.3.2 Third Party Application Porting Compatibility

The bidder should examine that application developed by third party software vendors are compatible to deploy on their platform. If there is anything which can't be port on their solution bidder should inform to MMRC and MMRC will coordinate with its ISV's in order to provide compatible code to their environment.

### 4.3.3 Third Party Application Porting Dependency Mapping

The bidder should prepare a detailed mapping of application and its dependency. If any application has any dependency and involves any cost, bidder should inform same to the MMRC.

## 4.4 Readiness and Risk Analysis

Since this is critical and larger environment, the bidder should study and submit a report of challenges endeavor from both an organizational readiness standpoint and a risk standpoint. Successfully identifying and mitigating both technical and organization risks is a critical factor is important for DR Solution. The bidder and MMRC both would require analyzing technical and organizational risks by using tools such as a SWOT (Strengths, Weaknesses, Opportunities, and Threats) analysis. Creating a comprehensive risk mitigation strategy outlining both preventative and compensatory actions will be necessary. Bidder shall carry out environmental feasibility study to identify environmental issues like corrosion etc at MMRC DR Premises and shall implement appropriate solution to ensure smooth and zero-error performance of infrastructure.

## 4.5 Connectivity

The bandwidth connectivity of 10 Mbps required for MMRCL to use the applications from the Cloud site and to ensure connectivity between MMRC DC and proposed DR will be provided by the managed service provider as per the technical specifications. The managed service provider will be responsible for core infrastructure facility for provisioning of internet, point to point connectivity, including termination devices, network security in terms of Enterprise Class firewall and IPS/IDS.

## 4.6 Data Center Site at MMRC

- The service provider shall Configure and Monitor DC Site at MMRC Premises and provide timely alerts for any issue via SMS, Email and Calls to contact persons of IT Department designated by MMRC.
- Review and suggest modification in Disaster recovery plans and guidelines for MMRCL providing details of:
  - The key persons to be contacted during the disaster
  - The various activities to be done by vendor and MMRCL for complete operations from DR site and restoration of operations to main production (cloud) site
- Service Provider shall provide standard operating procedures for smooth running and maintenance of Data Center site at MMRC.
- Service Provider shall co-ordinate with MMRC team and assist in Issue Resolution at Data Center Site at MMRC
- Service Provider shall co-ordinate with existing MMRC vendors for configuration of Data Center Site at MMRC.

## 4.7 Roles and Responsibilities of Service Provider

The service provider will be responsible for providing a tier 3 or above Cloud site within India.

- The Cloud site within India must be as per parameters mentioned in the Pre-Qualification criteria.
- Service Provider shall provide Single Point of Contact for all communication, resolution of issues and support required for smooth functioning of MMRC DC and proposed cloud DR at MMRC.
- The service provider shall develop, prepare and provide a Cloud Solution Implementation Plan. The Implementation Plan shall have the detailed design, specifications, drawings and schedule along with inspection and test plan, risk matrix and risk mitigation strategy, training material and documentation for all deliverables.
- Service Provider shall provide services comprising of, but not limited to, below items
  - Operating System Management
  - Network Management
  - Security Management
  - Storage Management
  - Backup Management
  - Disaster Recovery Management
- The service provider shall provision the cloud infrastructure, as and when ordered by MMRCL, as per scope of work defined in subsequent sections.
- Responsible for the replication of data between the proposed DR site and Data Center of MMRCL. The service provider will be responsible for commissioning the bandwidth, as

required by MMRCL, for replication of data and the SLA for the replication of data will be attributed to the service provider.

- The solution is envisaged for application level recovery scalable to site level recovery based on the impact of the disaster.
- The FMS provider and application development teams will support the Cloud Service provider during the deployment of the applications at the Cloud Solution site.
- Network setup (including switches, routers and firewalls) and uninterrupted network availability through a network link dedicated for connecting between the main DC site and DR site.
- Shared storage sizing for Cloud Hosting requirements.
- Necessary support in bringing the machines to login level in case of disaster / DR drills
- Provisioning, configuring and managing FC-IP router for DC to DR replication in case the proposed solution requires FC-IP router.
- Support during the recovery operations of data to and from DC-DR site.
- Ensuring related DNS changes for private WAN and internet, application availability and integrity, and database synchronization with application at DR site.
- 24x7x365 support for Hardware restoration (from self and OEMs used), managed hosting support (including L1, L2, and L3 support), Uptime commitment up to OS levels, managed & monitored backup and backup retention (as per period required by MMRCL), OS provisioning & management, dedicated security services operations, etc.
- Monitoring and maintenance reports over a monthly basis and as and when required.
- 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.
- Support in audit of the entire system on a yearly basis.
- On expiration / termination of the contract, handover of complete data in the desired format to MMRCL which can be easily accessible and retrievable.
- Compliance process to the defined international standards and security guidelines such as ISO 27001, ISO 20000, ITIL etc., for maintaining operations of cloud and ensuring privacy of MMRCL data. For the same an audit will have to be conducted on a periodic basis.
- The Cloud infrastructure and MMRCL data must be maintained ONLY at the location of the identified Cloud Hosting site. Data can only be moved to other site in case of any emergency with prior approval of MMRCL concerned authority.
- The bandwidth required for MMRCL to use the applications from the Cloud site will be provided by the service provider as per the technical specifications. The service provider will be responsible for core infrastructure facility for provisioning of internet, point to point connectivity, including termination devices, network security in terms of Enterprise Class firewall and IPS/IDS.
- Scaling the server and storage infrastructure up or down based on the needs of MMRCL.

- In case of reverse replication, since the DR site would be acting as main site, all the necessary support to run the environment has to be provided by the service Provider.
- Reverse Replication is necessary and envisaged when the DR site is acting as the main site. The solution should ensure consistency of data in reverse replication till the operations are not being established at the Cloud site. The RPO would be applicable in reverse replication also. The entire data should be made available for restoration at Primary Data Centre.
- MMRC shall have sole propriety rights for data stored in Cloud Environment at all times.
- It will be the Service Provider's responsibility to ensure that back up data is in a format that is restorable at Cloud Site or DR Site.

## 4.8 Security Requirements

- Identity and Access Management (IAM) that allows controlling the level of access to the users to the Service Provider's infrastructure services. With IAM, each user can have unique security credentials, eliminating the need for shared passwords or keys and allowing the security best practices of role separation and least privilege.
- Secure Access – Customer access points, also called API endpoints, to allow secure HTTP access (HTTPS) so that the Agencies can establish secure communication sessions with Cloud services using Secure Sockets Layer (SSL)/Transport Layer Security (TLS).
- Virtual Private Cloud with Private Subnets and Built-in Firewalls to control how accessible the instances are by configuring built-in firewall rules
- Multi-Factor Authentication (MFA)
- Data Encryption – Client Side and / or Server Side Encryption as required
- Dedicated Network Connection using industry-standard 802.1q VLANs
- Dedicated, Hardware-Based Crypto Key Storage Option for using Hardware Security Module (HSM) appliances
- Centralized Key Management
- DDoS Protection
- Service Provider should offer Dedicated application layer (Layer-7) security & user control platform which should be able to identify & prevent known & unknown threats (in real time basis) covering the related in-scope applications running on the network. The proposed solution should therefore integrate the user's identity repository (across all entities) to enforce authorized access to the related in-scope applications. The solution must be designed to ensure that the performance of the overall applications is not impacted due to the implementation of the security solutions and the management console should be same for this offering.
- The solution should offer application control, user based control, host profile, threat prevention, Anti-virus, file filtering, content filtering, QoS and scheduling capabilities in primary DC & DR site.

- Service Provider should offer SSL VPN solution which will be 100% client less/client based for accessing web based and TCP based application. SSL VPN solution must provide machine authentication based on combination of HDD ID, CPU info and OS related parameters to provide secure access to applications
- The proposed solution must support on appliance Per policy SSL and SSH decryption for both inbound and outbound traffic.
- Should support creation of C&C signatures based on IP, URL and DNS and content based AV signatures to block all the variants.
- It should have capability to blocks malware and its variants based on content based signatures also for malwares.
- The proposed solution should provide visibility into unknown threats, with the collective insight. It should correlate and gains intelligence from sandbox services, URL filter services, own research team, artifact-level statistical analysis and third-party feeds, including closed and open source intelligence.
- The solution should have provision to extend beyond the network, so that no application or attached device should be trusted. Instead of monitoring for patterns or malicious behaviours, or whitelisting applications, an advanced endpoint protection should persistently enforce the Zero Trust model on endpoints.
- The proposed solution must be in the Leader's quadrant in Gartner Magic Quadrant of Enterprise Firewalls for the last 3 years- 2016, 2015 and 2014.
- The solution should be capable to identify and prevent in-progress phishing attacks by controlling sites to which users can submit organization credentials based on the site's URL category thus blocking users from submitting credentials to untrusted sites while allowing users to continue to submit credentials to organization and sanctioned sites.
- The proposed solution shall provide sandbox behavior based inspection and protection of unknown viruses and zero-day malware for any application and protocol (not limited to HTTP, SMTP, FTP) and the solution shall be able to provide automated signature generation for discovered zero-day malware and the solution should ensure the delivery of the signature in 5 mins from the time of detection. The analysis has to be done on premise and data should not go to cloud for analysis.
- The lateral traffic between the virtual machines should get the same type of security as for north south traffic using virtual next generation security platform.
- Service Provider should offer dedicated appliance based DDOS solution (not integrated on firewall and any other network device) with multi-tenant support for department vide policy enforcement and monitoring
- Solution should detect and mitigate application layer DDOS protection for HTTP GET flooding, HTTP post flooding, HTTPS flooding, DNS flooding, DNS amplification, NTP amplification and other IP and TCP based attacks. support netflow v5, netflow v9, sflow v4, sflow v5, netstream v5, ipfix with out-of-line and inline deployment

- Security Incident and Event Management (SIEM) tool offered in SaaS based model, which correlates the event logs and alerts from multiple network devices and servers in near real time
- End point Antivirus and Antimalware, zero day protection for all mission critical servers / Virtual Machines
- Solution should provide security service for the intelligence, analytics, and context required to understand which attacks require immediate response, as well as the ability to make indicators actionable and prevent future attacks. It should be capable of integrate with Third-party open-source application that streamlines the aggregation, enforcement and sharing of threat intelligence
- Solution should have capabilities to analyse and correlating threat intelligence. For identified high-priority attacks, solution should enable organization to find related indicators of compromise (IOCs) and export them from the service so that organization can take immediate and decisive action to prevent threats and mitigate potential impact. It should allow IOC to be exported to external data which can be automatically integrated with enforcing points like Next gen firewalls.
- Service Provider should offer Web application firewall which will address Open Web Application Security Project (OWASP) Top Ten security vulnerabilities such as SQL Injection, Cross-Site Scripting (XSS), nonstandard encoding and Session Management. Protection from CSRF attacks by Adding a CSRF token to application responses and blocking of POST requests with a missing or incorrect CSRF token
- App firewall should have capability to scan source code using static analyzers (not dynamic scanners) and deploy patches locally. The solution is required to provide SAST, DAST and IAST approaches to application testing Support PHP, C#, Java and other web based applications
- Vulnerability testing on a half yearly basis. Reporting of the same on a half yearly basis
- Secure access to MMRC's infrastructure by Service Provider's authorized administrators via Privilege Infrastructure Management solution, that offer Identity, Authentication and Role based access to customer's Infrastructure
- The MSP shall procure and implement the following security solutions provided by third party:
    - Anti-Virus for the virtual machines
    - Host Intrusion Detection System
    - Web Application Firewall to help protect web applications from common web attacks such as SQL injection or cross-site scripting
    - SIEM to monitor the security incidents

## 4.9 Audit and Governance Requirements

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

- View into the performance and availability of the cloud services being used, as well as alerts that are automatically triggered by changes in the health of those services.
- Event-based alerts, to provide proactive notifications of scheduled activities, such as any changes to the infrastructure powering the cloud resources.
- System-wide visibility into resource utilization, application performance, and operational health through proactive monitoring (collect and track metrics, collect and monitor log files, and set alarms) of the cloud resources.
- Review of auto-scaling rules and limits.
- Logs of all user activity within an account. The recorded information should include the identity of the API caller, the time of the API call, the source IP address of the API caller, the request parameters, and the response elements returned by the cloud service. This is required to enable security analysis, resource change tracking, and compliance auditing.
- Ability to discover all of the provisioned resources and view the configuration of each. Notifications should be triggered each time a configuration changes, and Agencies should be given the ability to dig into the configuration history to perform incident analysis.
- Monitoring of cloud resources with alerts to customers on security configuration gaps such as overly permissive access to certain compute instance ports and storage buckets, minimal use of role segregation using identity and access management (IAM), and weak password policies.
- Automated security assessment service that helps improve the security and compliance of applications deployed on cloud by automatically assessing applications for vulnerabilities or deviations from best practices. After performing an assessment, the tools should produce a detailed list of security findings prioritized by level of severity.

## 4.10 Implementation Plan

The bidder should prepare and submit a detailed plan during execution of order with following details:

### 4.10.1 Consolidated Analysis of existing hardware:

Mapping of detailed hardware at primary site and DR site should be prepared with detailed analysis including following parameters:

- CPU calculations
- RAM calculations
- Disk calculations
- Network interfaces requirement

- Network throughput requirement
- Backup requirement

### 4.10.2 Virtual Cloud Deployment

The solution should be deployed to offer minimum RPO and RTO. (Pilot-Light for Quick Recovery, Warm Standby for further reduced recovery time, and Multi-Site Solution Deployment for active-active deployment as per the requirements of the project and the design of the application being migrated to cloud.)

Detailed planning of Virtual Private Cloud deployment and configuration should be submitted to MMRC. The configuration planning should include following details.

- Network architecture planning
- Firewall configuration planning.
- VLAN configuration planning
- IP address planning
- Subnet planning and routing planning
- Backup methodology
- Failover mechanism for replication links

### 4.10.3 System Planning:

Once the architecture is ready and the resources are ready to be provisioned on Cloud, the bidder should prepare detailed plan of system planning. This planning would require following details.

- On line and full off line backup of existing system.
- Notification of downtime to end users.
- System export window
- Replication tool configuration
- Transfer time of data from DC to DR
- Data restoration at DR side.
- Data Sync times and dependencies if any
- Switching on DC servers
- Notifying end users.
- Coordination with other vendors

Detailed planning of Disaster Recovery deployment and configuration should be submitted to MMRC. The configuration planning should include following details.

- Network architecture planning including
  - VLAN configuration planning
  - IP address planning
  - Subnet planning and routing planning

- Firewall configuration planning
- Backup methodology
- Failover mechanism for replication links
- Business continuity Architecture planning

On acceptance of the Implementation Plan by MMRC, the service provider shall implement the cloud solution and offer for testing.

### 4.10.4 Testing Planning

Following cloud resource deployment/provisioning, the testing of the same at Cloud site becomes very important. Therefore the service provider must perform following testing:

#### 4.10.4.1 Functional Testing

Once system is exported, data is migrated to Cloud site and application started functioning, the functional testing of Application will be done by MMRC Team along with application vendors. The bidder requires to provide support and co-ordination in this case. MMRC and application vendors may perform following testing.

- Software Module testing as per functional requirement.
- User authentications testing.
- Users add/delete, reports generations
- Heavy application transactions on DR servers.
- Backup exports
- Backup restoration

#### 4.10.4.2 Data Integrity Testing

Data integrations will be very important factor in overall process. Since data will be replicated over same or cross platform including same database at both end, the data integrity testing would become crucial. Data integrity testing will include:

- Amount of data verification at both end.
- Table size and records testing.
- Users status at both end.
- Invoices/transactions verification at both ends.
- Data in log files.

#### 4.10.4.3 Business Continuity testing

To demonstrate how the application fails over when the primary site goes down. The testing should include the:

- Uninterrupted replication to DR servers.
- Lag in replication due to any unforeseen errors.

- Process of recovering from lags if any.
- Data integrity test of DR servers.

### 4.10.5 Service Maintenance

The bidder requires to maintain the resources provisioned on Cloud. On Day to day basis bidder should send the reports of:

- Network monitoring
- Security monitoring and analysis

If any application patch has to be applied, it will be applied by MMRC and its software application vendors.

### 4.10.6 Failover

In the event of a disaster, the system at Proposed Bidder's Data Center will be primary system. All users of Company will connect to Bidder's system through Internet link. Since the systems has been asked on virtual private cloud infrastructure, all systems should be auto scalable. Whenever load of users will grow, the systems should scale resources automatically in terms of RAM and CPU. The failover from Main DC to DR should be done through a proper DR announcement process which should be documented as part of BCP planning.

### 4.10.7 Restoration

Restoration provides an easy process for copying updated data from the DR server back to the DC server. Whenever main DC will be recovered and operational, the data from DR system to DC systems should be synchronized. Once this data is synchronized and verified, the switchover from DR system to DC system should be done. In that case all users will be accessing systems of main DC.

### 4.10.8 Implementation of Project

The Bidder's proposal shall specify the project management methodology which would be used for this infrastructure setup and ensure compliance to relevant standards so as to make this equivalent to a Tier III data center.

The responsibilities of the bidder during this project over its logical broad phases are outlined in the subsequent sub-sections. The ongoing responsibilities of bidder during the project are also outlined below.

The activities / deliverables mentioned below are not exhaustive. The Bidder is expected to complete all activities / provide deliverables required to build the infrastructure in line with the quality / service standards prevalent in the industry for such infrastructure

#### 4.10.8.1 Phase 1: Project Preparation

During the first phase of project, the Bidder should prepare the project charter. The Bidder should also provide assistance in outlining the solution deployment architecture with details of hardware and Operating system platform and disaster recovery architecture. Some of the important activities / deliverables during this phase would be

1. Project Management Plan

The Bidder should prepare the project management plan, which outlines the project objectives, timelines, project procedures and project organization and submit it to MMRC for approval.
The Project Management Plan should include at least the following:

- Detailed methodology for setting up the DR infrastructure, dependencies etc.
- Risk Management Plan
- Quality Management Plan
- Escalation Procedures
- Approval Procedures
- Training Strategy and Plan
- Performance / Final Acceptance Test Plan for all components of the DR Solution.

2. Training Strategy

MMRC believes that key to successful implementation will be the Bidder's ability to train MMRC's staff in the operation of the proposed infrastructure:
As a part of the training strategy the Bidder should provide the following information:

- The facilities, support materials and program including mode of training (standard/ self-paced) provided for training the users in using the system.
- List of training areas for training to be provided to MMRC identified personnel and technical team.
- Training infrastructure required and expectations from MMRC , if any
- Duration and frequency of training

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

3. Project Plan

The Bidder shall develop a detailed Project Plan. The Project Plan shall amongst other functions, detail all tasks including but not limited to the task / person in charge for the execution of the task/ effort resource allocation. This information shall be provided in the form of a detailed Gantt chart. The Project Plan shall also detail all milestones and indicate when the required deliverable / documentation will be available to MMRC. This plan will be discussed with MMRC and finalized during the project preparation stage.

#### 4.10.8.2 Phase 2: Provisioning of Cloud Setup

The Bidder's team should study the existing infrastructure of MMRC and the requirements of the solution and build the Cloud infrastructure accordingly. DC Cloud Infrastructure readiness is the sole responsibility of the successful bidder. Interfaces with various agencies required to carry this out is the responsibility of the bidder.

Some of the important activities / deliverables during this phase would be:

- DR Site should confirm to Tier III Standards or above.
- Provisioning the resources on Cloud

#### 4.10.8.3 Phase 3: Commissioning, Testing and Training

During this phase of project, the Bidder will establish and commission the systems as per the specifications. The Bidder team will carry out the required customization / clustering / virtualization of servers to meet the requirements. Bidder should pass the configured system through its own internal quality processes and provide the compliance reports to the MMRC team. Training will also form part of this phase.

#### 4.10.8.4 Phase 4: Post Go Live Support

Bidder should provide post- Go Live support & DR Services support for entire contract period of five years as applicable. The support should be provided through help-desk support mechanism as defined below. It is assumed that the entire system would be stabilized at the end of post Go Live support.

#### 4.10.8.5 Help Desk Support

Bidder is required to create and maintain a Help Desk / telephonic number that will resolve problems and answer queries related to disaster recovery site and its equipment supplied by the bidder.

The help desk support to users shall be provided on 24x7x365 basis over telephone, chat and ticketing system. The details regarding telephonic, chat & ticketing support will be carefully considered, as this will have effect on the support response to MMRC system end-users. The Bidders response and resolution time will be the basis for end- user support time in MMRC‟s service level agreements with the Bidder.

### 4.10.9 Documentation

This documentation should be submitted as the project undergoes various stages of implementation. Indicative list of documents include:

- Detailed Project Plan
- Project Management Plan

- Training Material should be provided which shall include the presentations used for trainings and also the required relevant documents for the topics being covered.

The selected bidder shall document all the installation and commissioning procedures and provide the same to MMRC within one week of the commissioning of the DR Site. The selected bidder shall provide manuals for configuring DC Infrastructure. The selected bidder shall be responsible for documenting configuration of all devices / equipment and keeping back up of all configuration files, so as to enable quick recovery in case of failure of devices.

## 4.11 Project Timelines and Payment Terms

T= Issuance of LOA

| Sr. | Milestone | Deliverables | Timelines | Payment Terms * |
|---|---|---|---|---|
| 1 | Acceptance of LoI/Work Order/Contract (whichever is earlier) | Signed Contract & PBG of 10 % of total contract value | Project Start Date (T)* | Nil |
| 2 | Project Implementation Plan | Project kick off meeting, Project Inception Report covering approach & Project Plan | T + 2 Weeks | Nil |
| **A) Design , Configuration, Testing, Installation and Setup** | | | | |
| 3 | Network /Communication Links | Design , Configuration, Testing, Installation and Setup of ILL Connectivity as required | T+ 1 month | Nil |
| 4 | Cloud Solution Implementation and Migration | Provisioning of the cloud resources and Migration of the application on new Cloud Environment | T + 2 months | Nil |
| 5 | Operational Acceptance and Go-Live | User Acceptance Test Report, Operational Acceptance Report, Go-Live report | T+3 months | Nil |
| **B) Cloud Operation and Management (During O&M Period)** | | | | |
| 6 | Cloud Service Components offered | Cloud Resources Provisioning and Various MIS and Helpdesk Reports as described in this tender | As Required by MMRCL | Quarterly payments (QP) at end of quarter, on usage basis, after deducting all applicable penalties |

- No Advance payment against Purchase Order or Work order.
- All payment shall be released after submission of bills for quarterly period.
- Payment shall be made only for actual services, components utilized on hourly, monthly basis during quarter by MMRC.

### 4.11.1 Contract Period

The contract will start as per the date of award of the work order and will be valid for 5 years post Go-Live. The rates quoted will be valid for contract duration.

### 4.11.2 Specifications and Requirements

#### 4.11.2.1 Data Center Facility Requirement

MMRC seeks a data center facility that meets the following requirements. The requirements set forth below are intended to serve as a baseline reference only. Offers shall submit detailed descriptions of their data center facility.

- **Data Centre** : Cloud Services must be offered from a Data Center that is conforming to Tier III standards or above
- **Cloud Hosting**: MMRC looking for a stable, scalable and secured cloud infrastructure. In case, in future MMRC want same cloud infrastructure should be used as a production site. So proposed cloud platform should be horizontal and vertical scalable.
- **Reporting**: CSP should provide several reports wrt utilization and performance.
- **Availability**: uptime / availability of compute (99.5%) and Storage (99.5%)
- **Industry Standards**: MMRC seeks a data center complaint with industry standards as defined by (but not limited to) ISO 27001 / ISO 27018
- **RTO** <= 2 hours
- **RPO** <= 30 mins

| Sr. No | Description | Compliance (Y / N) | Remarks |
|---|---|---|---|
| | **Architectural** | | |
| **1** | Data center with a total built-up area | | |
| **2** | Data Center Tier Level | | |
| **3** | Active Capacity of component to support the IT load | | |
| **5** | Distribution paths | | |
| **6** | Double wall with cavity | | |
| **7** | Support Space to Raised- Floor Ratio | | |
| **8** | Raised-Floor Height (typical) | | |
| **9** | Floor Loading lbs./ft. (typical) | | |
| **10** | Annual Site-Caused, End-User Downtime (based on field data) | | |
| | **Electrical** | | |

| | | | |
|---|---|---|---|
| **1** | Number of power source through which power coming to data center | | |
| **2** | UPS Capacity – include battery runtime at full load. Verify full capacity is dedicated to the data center. | | |
| **3** | UPS Redundancy – N, N+1, 2N. | | |
| **4** | Electrical Power Distribution from UPS to IT Racks. Include method, strategy, voltage, redundancy, etc. | | |
| **5** | Deployment of Power Monitoring System in Data Center | | |
| **6** | Generator – Capacity & Current load | | |
| **7** | Generator Redundancy – N, N+1, 2N | | |
| | **Cooling System** | | |
| **1** | Mechanical heat rejection design/strategy – water-cooled chiller, air-cooled chiller, air cooled | | |
| **2** | Cooling Redundancy in data center – N, N+1, 2N. | | |
| **3** | Temperature maintain in data center | | |
| **4** | HVAC Monitoring systems deployed in data center | | |
| | **Fire Suppression** | | |
| **1** | Fire detection system deployed in data center | | |
| **2** | Fire suppression system deployed in data center | | |
| **3** | Firewall detection and control panel deployed in data center | | |
| | **Security** | | |
| **1** | Customer Access – Please indicate if 24x7. If not, please provide onsite availability and after hours response times | | |
| **2** | Onsite Security Staff – Please indicate if 24x7. If not, please provide onsite availability and after hours response times | | |
| **3** | Onsite Tech Staff – Please indicate if 24x7. If not, please provide onsite availability and after hours response | | |
| | times | | |
| **4** | Visual ID Required for Entry? | | |
| **5** | Means of controlled access – Access Card, Biometric, etc. | | |
| **6** | Video Surveillance System | | |
| | **Telecommunications** | | |
| **1** | Number of Internet Service Providers available at Data Center | | |
| **2** | Aggregated bandwidth available at Data Center | | |

| | | | |
|---|---|---|---|
| **3** | BGP4 routing protocol to route internal OSPF path to ISP | | |
| **4** | BGP peering for IPv4 as well as IPv6 network to provide IPv6 IP addresses. | | |
| **5** | BGP peering with National Internet exchange of India to router all domestic traffic through local exchange. | | |
| **6** | Tool to monitor incoming and outgoing traffic and check the link status. | | |
| | **Service Level Agreements** | | |
| **1** | Please describe your existing customer SLA's. Do you provide at least 99.5% availability? | | |
| **2** | 24 x 7 L1, L2, L3 support through Phone, Chat and Ticket Support | | |

### 4.11.2.2 Functional Requirement Specifications for Cloud Services

The Implementing Agency shall be responsible for provisioning the underlying system software, infrastructure, bandwidth, and cloud services for deployment and hosting of the application. While the minimum required compute, storage is provided in the RFP, it is expected that compute, storage, and bandwidth requirements may be auto-scaled (additional capacity based on the demand and auto-scaling rules) over the period of the contract in line with the transaction load to meet the SLA requirements. The application must be architected and designed to leverage the cloud characteristics such as rapid elasticity and handle transient and hardware failures without downtime. In addition to the production environment, the Implementing Agencies shall also provision for the test and training environments on the cloud.

The Implementing Agencies will be responsible for adequately sizing the necessary compute, memory, and storage required, building the redundancy into the architecture (including storage) and load balancing to meet the service levels mentioned in the RFP. While the initial sizing & provisioning of the underlying infrastructure (including the system software and bandwidth) may be carried out for the first year; subsequently, it is expected that the Implementing Agency, based on the growth in the user load (peak and non-peak periods; year-on-year increase), will scale up or scale down the compute, memory, storage, and bandwidth requirements to support the scalability and performance requirements of the solution and meet the SLAs

The solution should be architected to run on cloud services offered from multiple data center facilities to provide business continuity with no interruptions in case of any disruptions / disaster to one of the data center facility. In case of failure, automated processes should move customer data traffic away from the affected area. Applications should be deployed in an N+1 configuration, so that in the event of a data center failure, there is sufficient capacity to enable traffic to be load balanced to the remaining sites. The Cloud Service Provider should provide adequate bandwidth between the Data Center Facilities to provide business continuity.

The public facing services shall be deployed in a zone (DMZ) different from the application services. The Database nodes (RDBMS) should be in a separate zone with higher security layer.

The UAT and training portals on the cloud should be separate from the production portal in a different VLAN than the production environment and setup such that users of the environments are in separate networks. The cloud services shall comply with the following requirements:

### 1. Regulatory Requirements

| | Requirement | Description | Compliance (Y/N) | Remarks |
|---|---|---|---|---|
| 1. | Data center and Disaster recovery locations in following geographies – India | Cloud provider should offer cloud services (IAAS , PAAS , SAAS) within India and Disaster recovery site too should be in India | | |
| 2. | Maintain and ensure data locality | Cloud provider should ensure that customer data resides only in the Region they specify. | | |
| 3. | Protect your applications from the failure of a single location | Cloud provider should offer data centers engineered to be isolated from failures in other data centers, and to provide network connectivity to other data centers within the country. | | |

### 2. Compute

| | Requirement | Description | Compliance (Y/N) | Remarks |
|---|---|---|---|---|
| 4. | Compute instances –<br>• General Purpose<br>• Memory optimized<br>• Compute optimized | Cloud provider should offer the following instance types –<br>• General Purpose – optimized for generic applications and provides a balance of compute, memory, and network resources.<br>• Memory optimized – optimized for memory applications | | |

| | | | | |
|---|---|---|---|---|
| | • Storage optimized | • Compute optimized – optimized for compute applications<br>• Storage optimized – include very fast/large amount of local storage for NoSQL databases and Hadoop | | |
| 5. | Compute instances – Burstable performance | Cloud provider should offer instances that provide a baseline level of CPU performance with the ability to burst above the baseline. | | |
| 6. | Compute instances – Management | Cloud provider should offer instances that can be managed by customer using Self-service portal at no additional cost. | | |
| 7. | OS Support – Linux | Cloud provider should be able to support following Linux distributions - (Red Hat, SUSE, Ubuntu, CentOS, and Debian) | | |
| 8. | OS Support – Windows | Cloud provider should be able to support the Windows Server versions (Windows Server 2016, 2012, Windows Server 2008) | | |
| 9. | Resize virtual Machines seamlessly | Customer must be able to specify and modify server configuration (including CPU, memory, storage) parameters seamlessly. | | |
| 10. | Local disk/Instance store | Cloud service should provide local storage for compute instances to be used for temporary storage of information that changes frequently. | | |
| 11. | Provision multiple concurrent instances | Cloud service must offer self-service provisioning of multiple instances concurrently either through a programmatic interface (API/CLI) or through a management console. | | |
| 12. | Instance affinity - logical grouping of instances within a single data center | Customer should be able to logically group instances together for applications that require low network latency and/or high network throughput. | | |
| 13. | Instance anti-affinity -two or more instances hosted in different data centers | Customer should be able to split and host instances across different physical data centers within India to ensure that a single physical datacenter failure event does not take all instances offline. | | |

| | | | | |
|---|---|---|---|---|
| 14. | Auto Scaling support | Cloud service should be able to automatically increase the number of instances during demand spikes to maintain performance and decrease capacity during lulls to reduce costs. | | |
| 15. | Bring your own image/Instance Import | Customer should be able to import their existing image and save it as a new, privately available image that can then be used to provision instances in the future. | | |
| 16. | Export Instance Image | Cloud service must support the ability to take an existing running instance or a copy of an instance and export the instance into an Interoperable VMDK or VHD image format. | | |
| 17. | Instance maintenance mitigation | Cloud service must be architected in such a way to avoid instance outages or downtime when the provider is performing any kind of hardware or service maintenance. | | |
| 18. | Instance failure recovery | Cloud service must be architected in such a way to automatically restart instances on a healthy host if the original physical host fails. | | |
| 19. | Instance restart flexibility | Cloud provider must be able to schedule events for customer's instances, such as a reboot, stop/start, or retirement. Depending on the event, customer might be able to take action to control the timing of the event. | | |
| 20. | Support for Docker containers | Cloud service should support containers, including Docker and/or other containerization platforms. | | |
| 21. | Highly scalable, high performance container management service | Cloud provider should offer a highly scalable, high performance container management service. | | |
| 22. | Event-driven computing that runs code in response to events | Cloud service should be able to run customer code in response to events and automatically manage the compute resources. | | |
| 23. | License portability and | Cloud provider should offer license portability and support for Microsoft | | |

| | | | | |
|---|---|---|---|---|
| | support – Microsoft | apps like SQL Server and SharePoint Server. | | |
| 24. | License portability and support – Oracle | Cloud provider should offer license portability and support for Oracle apps like Oracle Database 11g. | | |
| 25. | License portability and support – SAP | Cloud provider should offer license portability and support for SAP apps like HANA. | | |
| 26. | License portability and support – IBM | Cloud provider should offer license portability and support for IBM apps like DB2 and Websphere. | | |
| 27. | Pay-as-you-go pricing | Cloud provider should offer a simple pay-as-you-go pricing where customers can pay for compute capacity by the minute with no long-term commitments. | | |

### 3. Service Provisioning

| | Requirement | Compliance (Y/N) | Remarks |
|---|---|---|---|
| 28. | The CSP should offer cloud service provisioning portal for PURCHASER in order to provision cloud services either via portal, mobile app or automated using API. | | |
| 29. | Cloud service provider should enable to provision cloud resources through self service provisioning portal. | | |
| 30. | CSP should enable to provision cloud resources from application programming interface (API). | | |
| 31. | The user admin portal should be accessible via secure method using SSL certificate. | | |
| 32. | Should be able to create, delete, shutdown, reboot virtual machines from provisioning portal. | | |
| 33. | Should be able to provision additional resources from provisioning portal as and when require. | | |
| 34. | Should be able to take snapshot of virtual machines from provisioning portal. | | |
| 35. | Should be able to size virtual machine and select require operating system | | |

| | | | |
|---|---|---|---|
| | when provisioning any virtual machines. | | |
| 36. | Should be able to predict his billing of resources before provisioning any cloud resources. | | |
| 37. | Should be able to set threshold of cloud resources of all types of scalability. | | |
| 38. | Should be able to provision all additional storages require for cloud services. | | |
| 39. | Should be able to provision any kind of resources either static or elastic resources. | | |
| 40. | Should be able to take console of cloud virtual machines from portal to perform any operations. | | |
| 41. | Should get list of all cloud resources from provisioning portal. | | |
| 42. | Should be able to set the scaling parameters like in case of horizontal scaling, | | |
| 43. | Should be able to set percentage / quantity of RAM consumption to trigger new virtual machines. | | |
| 44. | Should be able to set percentage / quantity of CPU consumption to trigger new virtual machines. | | |
| 45. | Should be able to set percentage / quantity of network bandwidth to trigger new virtual machines. | | |
| 46. | Should be able to set port on which horizontal scaling will work. | | |
| 47. | Should be able to set minimum and maximum number of virtual machines which will be automatically provisioned as part of horizontal scaling to handle spike in load. | | |
| 48. | The cloud virtual machine created by portal should be have at-least two virtual NIC cards. One NIC card should be used for internet traffic while other should be used for internal service traffic. | | |

| | | | |
|---|---|---|---|
| 49. | The Cloud Service should be able to provision additional Software from the market place. | | |

### 4. Networking

| | Requirement | Description | Compliance (Y/N) | Remarks |
|---|---|---|---|---|
| 50. | Multiple network interface/instance | Cloud service should be able to support multiple (primary and additional) network interfaces. | | |
| 51. | Multiple IP addresses /instance | Cloud service should be able to support multiple IP addresses per instance. Use cases include hosting multiple websites on a single server and network appliances (such as load balancers) that have multiple private IP addresses for each network interface. | | |
| 52. | Ability to move network interfaces and IPs between instances | Cloud service should support the ability to create a network interface, attach it to an instance, detach it from an instance, and attach it to another instance. | | |
| 53. | Enhanced networking support | Cloud service should support capabilities such as single root I/O virtualization for higher performance (packets per second), lower latency, and lower jitter. | | |
| 54. | Network traffic logging - Log traffic flows at network interfaces | Cloud service should support capturing information about the IP traffic going to and from network interfaces. | | |
| 55. | Auto-assigned public IP addresses | Cloud service should be able to automatically assign a Private or public IP to the instances. | | |
| 56. | IP Protocol support | Cloud service should be able to support multiple IP protocols, including TCP, UDP, and ICMP protocols. | | |
| 57. | Use any network CIDR, including RFC 1918 | Cloud service should be able to support IP address ranges specified in RFC 1918 as well as publicly routable CIDR blocks. | | |

| | | | | |
|---|---|---|---|---|
| 58. | Static public IP addresses | Cloud provider must support IP addresses associated with a customer account, not a particular instance. The IP address should remain associated with the Virtual Machine until released explicitly. | | |
| 59. | Auto-created default virtual private network | Cloud service should be able to create a default private network and subnet with instances launching into a default subnet receiving a public IP address and a private IP address. | | |
| 60. | Subnets within private network | Customer should be able to create one or more subnets within private network with a single Classless Inter-Domain Routing (CIDR) block. | | |
| 61. | Subnet level filtering (Network ACLs) | Cloud service should support subnet level filtering – Network ACLs that act as a firewall for associated subnets, controlling both inbound and outbound traffic at the subnet level. | | |
| 62. | Ingress filtering | Cloud service should support adding or removing rules applicable to inbound traffic (ingress) to instances. | | |
| 63. | Egress filtering | Cloud service should support adding or removing rules applicable to outbound traffic (egress) originating from instances. | | |
| 64. | Disable source/destination checks on interfaces | Cloud service should support the ability to disable source/destination check on network interfaces. By default, compute instances perform source/destination checks. | | |
| 65. | Configure proxy server (NAT instance) at network level | Cloud service should support NAT instances that can route traffic from internal-only instances to the Internet. | | |
| 66. | Site-to-site managed VPN service | Cloud service should support a hardware based VPN connection between the cloud provider and customer data center. | | |

| | | | | |
|---|---|---|---|---|
| 67. | Virtual Network Peering | Cloud service should support connecting two virtual networks to route traffic between them using private IP addresses. | | |
| 68. | Multiple VPN Connections per Virtual Network | Cloud service should support creating multiple VPN connections per virtual network | | |
| 69. | BGP for high availability and reliable failover | Cloud provider should support Border Gateway Protocol. BGP performs a robust liveness check on the IPSec tunnel and simplifies the failover procedure that is invoked when one VPN tunnel goes down. | | |
| 70. | Private connection to customer data centers | Cloud provider should support direct leased-line connections between cloud provider and a customer datacenter, office, or colocation environment, which in many cases can reduce network costs, increase bandwidth throughput, and provide a more consistent network experience than Internet-based connections. | | |
| 71. | DNS based global load balancing | Cloud service should support Load balancing of instances across multiple host servers. | | |
| 72. | Load balancing supports multiple routing methods | Cloud service should support multiple routing mechanism including round-robin, failover, sticky session etc. | | |
| 73. | Front-end Load Balancer | Cloud service should support a front-end load balancer that takes requests from clients over the Internet and distributes them across the instances that are registered with the load balancer. | | |
| 74. | Back-end Load Balancer | Cloud service should support an internal load balancer that routes traffic to instances within private subnets. | | |
| 75. | Health checks - monitor the health and performance of application | Cloud service should support health checks to monitor the health and performance of resources. | | |

| | | | | |
|---|---|---|---|---|
| 76. | Integration with Load Balancer | Cloud service should support integration with load balancer. | | |
| 77. | Low Latency | The CSP should be able to provide a 10GB network connectivity between the server if required. | | |

## 5. Storage – Block Storage

| | Requirement | Description | Compliance (Y/N) | Remarks |
|---|---|---|---|---|
| 78. | Support for storage allocated as local disk to a single VM | Cloud provider should offer persistent block level storage volumes for use with compute instances. | | |
| 79. | Storage volumes > 1 TB | Cloud provider should offer block storage volumes greater than 1 TB in size. | | |
| 80. | SSD backed storage media | Cloud service should support solid state drive (SSD) backed storage media that offer single digit millisecond latencies. | | |
| 81. | Provisioned I/O support | Cloud service 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. | | |
| 82. | Encryption using provider managed keys | Cloud service should support encryption of data on volumes, disk I/O, and snapshots using industry standard AES-256 cryptographic algorithm. | | |
| 83. | Encryption using customer managed keys | Cloud service should support encryption using customer managed keys. | | |
| 84. | Durable snapshots | Cloud service should support point-in-time snapshots. These snapshots should be incremental in nature. | | |
| 85. | Ability to easily share snapshots globally | Cloud Service should support sharing of snapshots across regions making it easier to leverage multiple regions for geographical expansion, data center migration, and disaster recovery. | | |
| 86. | Consistent Input Output per second (IOPS) | Cloud service should support a baseline IOPS/GB and maintain it consistently at scale | | |

| | | | | |
|---|---|---|---|---|
| 87. | Annual Failure Rates <1% | Cloud service should be durable and support annual failure rates of less than 1% | | |

## 6. Storage – Object Storage

| | Requirement | Description | Compliance (Y/N) | Remarks |
|---|---|---|---|---|
| 88. | Scalable object storage service | Cloud provider should offer secure, durable, highly-scalable object storage for storing and retrieving any amount of data from the web. | | |
| 89. | Low cost archival storage with policy support | Cloud provider should support an extremely low-cost storage service that provides durable storage with security features for data archiving and backup. | | |
| 90. | Data Locality | Cloud provider should provide a strong Datacenter location isolation, so that objects stored in a that datacenter never leave the datacenter unless customer explicitly transfers them to another Datacenter. | | |
| 91. | High-scale static web site hosting | Cloud service should be able to host a website that uses client-side technologies (such as HTML, CSS, and JavaScript) and does not require server-side technologies (such as PHP and ASP.NET). | | |
| 92. | Lower Durability offering | Cloud service should support a lower cost option for noncritical, reproducible data at lower levels of redundancy. | | |
| 93. | Strong Consistency | Cloud service should support read-after-write data consistency. | | |
| 94. | Accept large data loads through shipped physical media | Cloud provider should support moving large amounts of data into the cloud by bypassing the internet. | | |

## 7. Storage – File Storage

| | Requirement | Description | Compliance (Y/N) | Remarks |
|---|---|---|---|---|

| | | | | |
|---|---|---|---|---|
| 95. | Simple, scalable file storage service | Cloud provider should offer a simple scalable file storage service to use with compute instances in the cloud. | | |
| 96. | SSD backed storage media | Cloud service should offer SSD backed storage media to provide the throughput, IOPS, and low latency needed for a broad range of workloads. | | |
| 97. | Grow file systems to petabyte scale | Cloud service should support petabyte-scale file systems and allow thousands of concurrent NFS connections. | | |
| 98. | Consistent low latency performance (T50-T99) | Cloud service should support consistent low latency performance between 5-15 ms at any scale. | | |
| 99. | Scalable IOPS and throughput performance (/TB) | Cloud service should support scalable IOPS and throughput performance at any scale. | | |
| 100. | Fully elastic capacity (no need to provision) | Cloud service should automatically scale up or down as files are added or removed without disrupting applications. | | |
| 101. | Highly durable | Cloud service should be highly durable - file system object (i.e. directory, file, and link) should be redundantly stored across multiple data centers. | | |
| 102. | Read-after-write consistency | Cloud service should support read after write consistency (each read and write operation is guaranteed to return the most recent version of the data). | | |

## 8. Relational Database

| | Requirement | Description | Compliance (Y/N) | Remarks |
|---|---|---|---|---|
| 103. | Managed relational database service | Cloud provider should offer a service that makes it easy to set up, operate, and scale a relational database in the cloud. | | |
| 104. | Support for MySQL | Cloud service should support latest version of MySQL as a database engine. | | |
| 105. | Support for Oracle | Cloud service should support latest version of Oracle as a database engine. | | |

| | | | | |
|---|---|---|---|---|
| 106. | Support for Microsoft SQL Server | Cloud service should support latest version of SQL Server as a database engine. | | |
| 107. | Support for PostgreSQL | Cloud service should support latest version of PostgreSQL | | |
| 108. | Low latency, synchronous replication across multiple data centers in India | Cloud service should support synchronous replication of a primary database to a standby replica in a separate physical datacenter to provide data redundancy, eliminate I/O freezes, and minimize latency spikes during system backups. | | |
| 109. | Read Replica support | Cloud service should support read replicas that make it easy to elastically scale out beyond the capacity constraints of a single DB Instance for read-heavy database workloads. | | |
| 110. | Manual Failover | Cloud service should support a manual failover of the DB instance from primary to a standby replica. | | |
| 111. | Provisioned IO support | Cloud service should support the needs of database workloads that are sensitive to storage performance and consistency in random access I/O throughput. | | |
| 112. | Bring your own SQL, Oracle licenses | Cloud service should support customers who prefer to use their existing Oracle and SQL Server database licenses in the cloud. | | |
| 113. | Bring your own Windows / Linux Server licenses | Cloud service should support customers who prefer to use their existing Windows Server and Linux licenses in the cloud. | | |
| 114. | Cross Datacenter Snapshots | Cloud service should support copying snapshots of any size between different cloud datacenters for disaster recovery purposes. | | |
| 115. | Cross datacenter Read Replica | Cloud service should support creating multiple in-datacenter and across-datacenter replicas within India per database instance for scalability or disaster recovery purposes. | | |

| | | | | |
|---|---|---|---|---|
| 116. | High Availability | Cloud Service should support enhanced availability and durability for database instances for production workloads. | | |
| 117. | Point in time restore | Cloud service should support restoring a DB instance to a specific date and time. | | |
| 118. | User snapshots and restore | Cloud service should support creating a DB snapshot and restoring a DB instance from a snapshot. | | |
| 119. | Modifiable DB parameters | Cloud service should allow the DB parameter to be modified. | | |
| 120. | Monitoring | Cloud service should allow monitoring of performance and health of a database or a DB instance. | | |
| 121. | Encryption at rest | Cloud service should support encryption using the industry standard AES-256 encryption algorithm to encrypt data. | | |

## 9. Non-Relational Database

| | Requirement | Description | Compliance (Y/N) | Remarks |
|---|---|---|---|---|
| 122. | Scalable, fast and flexible NoSQL database service | Cloud provider should offer a fast and flexible NoSQL database service for applications that need consistent, single-digit millisecond latency at any scale. | | |
| 123. | Replication | Cloud service should support automatic replication of data across multiple physical datacenters in a region to provide high availability and data durability. | | |
| 124. | Performance/ Latency | Cloud service should support single-digit milliseconds (TP99) latencies at any scale. | | |
| 125. | Key-value Data Model support | Cloud service should support key value data structure where the primary key is the only required attribute for items in a table and uniquely identifies each item. | | |
| 126. | Document Data Model | Cloud service should support storing, querying, and updating JSON documents. | | |

| | | | | |
|---|---|---|---|---|
| | with JSON support | | | |
| 127. | Tunable scaling | Cloud service should support seamless throughput and storage scaling. | | |
| 128. | Secondary Indexes | Cloud services should support secondary indexes. Secondary indexes are indexes that contain hash or hash-and-range keys that can be different from the keys in the table on which the index is based. | | |
| 129. | Streams | Cloud service should support streams. Stream is an ordered flow of information about changes to items. | | |
| 130. | Cross region replication | Cloud Service should support cross-datacenters replication (within India) to automatically replication data across multiple datacenter. | | |
| 131. | Database triggers | Cloud Service should support database triggers - pieces of code that quickly and automatically respond to data modification in the tables. | | |
| 132. | Strong consistency, Atomic counters | Cloud service should support strong consistency for read operations to make sure users are always reading the latest values. | | |
| 133. | Integrated Monitoring | Cloud service should support monitoring of request throughput and latency for database tables, among other metrics. | | |
| 134. | Integration with data warehouse | Cloud service should support integration with a data warehouse for advanced business intelligence capabilities. | | |
| 135. | Hadoop Integration | Cloud service should support integration with a Hadoop framework to perform complex analytics on large datasets. | | |

### 10.Security and administration

| | Requirement | Description | Compliance (Y/N) | Remarks |
|---|---|---|---|---|
| 136. | Control access to your cloud resources at a granular level | Cloud provider should offer fine-grained access controls including, conditions like time of the day, originating IP address, use of SSL certificates, or authentication with a multi-factor authentication device. | | |
| 137. | Utilize multi-factor authentication | Cloud service should support multi-factor authentication. MFA requires users to prove physical possession of a | | |

| | | | | |
|---|---|---|---|---|
| | when accessing cloud resources | hardware or virtual MFA device by providing a valid MFA code. | | |
| 138. | Identify when an access key was last used to rotate old keys and remove inactive users | Cloud service should support reporting a user's access keys last use details. | | |
| 139. | Directory as a service | Cloud provider should support setting up a stand-alone directory in the cloud or connecting cloud resources with existing on-premises Microsoft Active Directory. | | |
| 140. | User and Group management | Cloud service should support features such as user and group management. | | |
| 141. | Integration with your existing on-premises Active Directory | Cloud service should integrate with existing on-premise Active Directory. | | |
| 142. | Self-service password reset for cloud users | Cloud service should allow users to reset their password in a self-service manner. | | |
| 143. | Dedicated, hardware security module (HSM) appliance | Cloud provider should offer HSM modules. | | |
| 144. | Managed service to create and control the encryption keys used to encrypt your data | Cloud provider should offer a service to create and control the encryption keys used to encrypt user data. | | |
| 145. | Audit of all action on keys | Cloud service should support auditing with features such as what request was made, the source IP address from which the request was made, who made the request, when it was made, and so on. | | |
| 146. | Key Durability | Cloud service should support durability of keys, including storing multiple copies to ensure keys are available when needed. | | |
| 147. | Web service to record API calls | Cloud provider should offer a service to record history of API calls and related events for a user account. | | |

| | | | | |
|---|---|---|---|---|
| | and deliver log files | | | |
| 148. | Receive notification of API activity | Cloud service should support notifications when new log files are available. | | |
| 149. | Durable and inexpensive log file storage | Cloud service should support storing log files in a durable and inexpensive storage solution. | | |
| 150. | Choice of partner solution | Cloud service should support a variety of 3rd party solutions. | | |
| 151. | Aggregation across multiple accounts and multiple datacenters (In India) for ease of use | Cloud service should support receiving log files from multiple regions and accounts to a single location for ease of use. | | |
| 152. | Managed service for resource inventory, configuration history & change notifications | Cloud provider should offer a service that provides resource inventory, configuration history, and configuration change notifications to enable security and governance. | | |
| 153. | Automatically records a resource's configuration when it changes | Cloud service should automatically record a resource configuration when it changes and make this information available. | | |
| 154. | Examine the configuration of your resources at any single point in the past | Customer should be able to obtain details of what a resource's configuration looked like at any point in the past using this cloud service. | | |
| 155. | Receive notification of a configuration change | Cloud service should notify every configuration change so customers can process these notifications programmatically. | | |
| 156. | Create and manage catalog of pre-approved services for use | Cloud provider should offer the ability to create and manage catalogs of IT services that are approved for use. | | |

## 11.Security and administration - Independent 3rd part Assurance Programs

| | Requirement | Description | Compliance (Y/N) | Remarks |
|---|---|---|---|---|

| | | | | |
|---|---|---|---|---|
| 157. | 3rd party Assurance Programs<br>ISO 27001 / ISO 27018<br>ISO 9001<br>PCI DSS Level 1<br>The Ministry of Electronics and Info Technology | Cloud provider should meet a broad set of international and industry-specific compliance standards | | |

## 12. Deployment and Management

| | Requirement | Description | Compliance (Y/N) | Remarks |
|---|---|---|---|---|
| 158. | Service to quickly deploy and manage applications in the cloud | Cloud provider should offer a service to quickly deploy and manage applications in the cloud by automatically handling the deployment, from capacity provisioning, load balancing, auto-scaling to application health monitoring. | | |
| 159. | Supported Platforms<br>Java<br>Python<br>Ruby<br>Google Go<br>.NET<br>PHP<br>Node.js | Cloud service should support a wide variety of platforms from Java and .NET to Google Go. | | |
| 160. | Supported OS<br>Windows<br>Linux<br>any OS in Docker | Cloud Service should support Windows, Linux, and Docker containers. | | |
| 161. | Deployment Mechanism<br>Git<br>Visual Studio<br>Zip<br>Eclipse | Cloud service should support various deployment mechanisms, including a Git repository, or an integrated development environment (IDE) such as Eclipse or Visual Studio. | | |

| | | | | |
|---|---|---|---|---|
| 162. | Support for SSL connections | Cloud service should support SSL connections. | | |
| 163. | Application source versioning | Cloud service should support application source versioning. This would be useful for applications that have been updated and need to be redeployed. | | |
| 164. | Auto scaling | Cloud service should support automatically launching or terminating instances based on the parameters such as CPU utilization defined by users. | | |
| 165. | Swap virtual IP between staging and production environments | Cloud service should support swapping IP addresses between staging and production environments so that a new application version can be deployed with zero downtime. | | |
| 166. | Integration with caching solution | Cloud service should be integrated with a caching solution such as Redis cache. | | |
| 167. | Service to create a collection of related resources and provision them using a template | Cloud provider should offer a service to create a collection of related resources and provision them in an orderly and predictable fashion using a template. | | |
| 168. | Allow parametrization and specific configurations | Cloud service should support parameterization for specific configuration. | | |

## 13. Application Service

| | Requirement | Description | Compliance (Y/N) | Remarks |
|---|---|---|---|---|
| 169. | Queueing service | Cloud provider should offer a fast, reliable, scalable, fully managed message queuing service. | | |
| 170. | Notification service | Cloud provider should offer a fast, flexible, fully managed push notification service that lets users send individual messages or to fan-out messages to large numbers of recipients. | | |
| 171. | Bulk email delivery service | Cloud provider should offer (through partners solution) a cost-effective outbound-only email-sending service. | | |
| 172. | Productivity Suite Service | Cloud Provider should provide Email , Video conferencing , portal and Productivity suite services | | |

## 14. Hybrid Integration

| | Requirement | Description | Compliance (Y/N) | Remarks |
|---|---|---|---|---|
| 173. | Virtual private networking connection to cloud resources | Cloud provider should be able to extend customer's data center to the cloud and enable communication with their own network over an IPsec VPN tunnel. | | |
| 174. | High speed, low latency, dedicated connectivity between on-premises & cloud | Cloud provider should provide mechanisms to establish private connectivity between the cloud environment and a customer datacenter, office, or colocation environment. | | |
| 175. | Automated VM import functionality | Cloud provider should allow customers to import VMs from a virtualization environment such as Citrix Xen, Microsoft Hyper-V, or VMware vSphere. | | |
| 176. | Automated VM migration functionality | Cloud provider should provide and allow customers Migration of instances to and from their on-premises virtualization environments. | | |

| | | | | |
|---|---|---|---|---|
| 177. | Integrate with on-premises Active Directory | Cloud service should integrate with existing on-premise Active Directory. | | |
| 178. | Use any IP address range, including RFC 1918 | Cloud service should be able to support IP address ranges specified in RFC 1918 as well as publicly routable CIDR blocks. | | |
| 179. | Highly durable, automatic data replication, and recovery service from on-premises | Cloud provider should offer a service to automatically replicate data from on-premises to cloud for disaster recovery purposes. | | |
| 180. | Backup service to back up on-premises servers | Cloud provider should offer a service with ability to take regular and scheduled back of on-premises servers. | | |
| 181. | Utilize multi-factor authentication when accessing cloud resources | Cloud service should support multi-factor authentication. MFA requires users to prove physical possession of a hardware (Mobile devices) or virtual MFA device by providing a valid MFA. | | |

## 15.Support

| | Requirement | Description | Compliance (Y/N) | Remarks |
|---|---|---|---|---|
| 182. | Service Health Dashboard | Cloud provider should offer a dashboard that displays up-to-the-minute information on service availability across multiple regions. | | |
| 183. | 365 day service health dashboard and SLA history | Cloud provider should offer 365 days' worth of Service Health Dashboard (SHD) history. | | |
| 184. | Monitoring Tools | Monitoring tools that will enable collection and tracking metrics, collection and monitoring log files, set alarms, and automatically react to changes in the provisioned resources. The monitoring tools should be able to monitor resources such as compute and other resources to gain system-wide visibility into resource utilization, application performance, and operational health. | | |

| | | | | |
|---|---|---|---|---|
| 185. | Audit Trail | Provide Audit Trail of the account activity to enable security analysis, resource change tracking, and compliance auditing | | |

## 16.SIEM (From Partners of Market Place)

| | Requirement | Compliance (Y/N) | Remarks |
|---|---|---|---|
| 186. | Should Supports root cause analysis with built-in intelligence. | | |
| 187. | Should Collects, consolidates, and analyzes logs and events from firewalls, IDS/IPS devices and applications, switches, routers, servers, operating system logs, and other applications. | | |
| 188. | Should blocks and quarantines malicious and suspicious activity, including inappropriate USB usage. | | |
| 189. | Provide real time intelligent analytical data from logs. | | |
| 190. | IT admins should get the log data displayed on the dashboard for better understanding on user activity network threats and event trends within a short span of time. | | |
| 191. | Provide real time intelligent analytical data from logs. | | |
| 192. | Easy & Scalable Log Collection, Universal log collection is possible from any source by agent base or agentless version. | | |
| 193. | All the intruders, unauthorized, accidental access to restricted objects in network can be track. File integrity monitoring should be possible. | | |
| 194. | Customizable IT Compliance schedule reporting | | |
| 195. | It should provide extraordinary customized regulatory compliance reports for various regulatory compliance standards, such as PCI DSS and FISMA. | | |
| 196. | Should provide Log & Event Manager which enables immediate respond to security, operational, and policy driven events using built-in active responses. | | |
| 197. | SIEM should be quick and simple to deploy. You should be up and auditing logs in no time using auto remote agent deployment model, Web based console, and intuitive interface. | | |

## 4.12 Change Management Workshops

- The service provider shall conduct training sessions, explaining features of the Cloud system and how to use these features for in case of any departmental requirement. The training material (master copy) will be provided by the solution provider. Hands on training sessions should be of about one day duration and shall be conducted. The training shall be provided by a trained & experienced professional having excellent communication skills. MMRCL will be providing desktops/OHP/necessary infrastructure to trainers. The training should be at no extra cost to MMRCL. The bidder will submit two hard copies of the orientation and technical training to MMRCL.
- The total users to be trained for each senior management orientation and technical session will be 50 users each.

| Sr. | Type of Training | Target Audience | No. of sessions (Batch size =20) | Duration per Session | Manual / Material Required? |
|---|---|---|---|---|---|
| 1 | Orientation | Senior Management | 1 per Quarter for 1st Year | 1 Day | Yes |
| 2 | Orientation | Senior Management | 1 per year for 2nd year onwards | 1 Day | Yes |
| 3 | Technical Session | Local Administrator , FMS Vendor, DR Vendor | 1 per Quarter for 1st Year | 2 Days | Yes |
| 4 | Technical Session | Local Administrator , FMS Vendor, DR Vendor | 1 per year for 2nd year onwards | 2 Days | Yes |

## 4.13 Functional Requirement Specifications (FRS) of Cloud Solution

The functional requirement specifications (FRS) of the cloud solution is described in Section 4.11.2. The bidder has to offer cloud solution as per the FRS.

## 4.14 Regulation, Licensing and Domain

The service provider shall arrange for all the necessary legal, regulatory and licensing clearances for the trouble free/hassle free operations of the Cloud services to MMRCL. All Licenses procured shall be in name of MMRC.

## 4.15 Commissioning

Commissioning of the System (or Subsystem if specified in the Contract) shall be commenced by the service provider:

- Immediately after the Go-Live Certificate is issued by MMRCL.
- as otherwise specified in the Technical Requirement or the Agreed and Finalized Project Plan;

## 4.16 Operational Acceptance

- Operational Acceptance shall commence on the system, once the system is commissioned to a period of maximum 30 days.
- Operational Acceptance will only be provided after cloud resources and provisioned and switchover testing (as applicable) has been completed. Switchover testing would include:
  - Switch over of application from DC to DR as per defined RTO and RPO
  - Switch over applications from DR to DC as predefined RTO and RPO
  - Complete Data Replication and Reverse Data Replication as per RPO
  - Fully functional application while DR site is operational as confirmed by MMRCL end users of application
- The service provider will have to facilitate the operational acceptance tests. Operational acceptance tests will be performed by MMRCL; however Service provider will have to facilitate operation acceptance during commissioning of the system (or subsystem[s]), to ascertain whether the system (or major component or Subsystem[s]) conforms to the scope of work, including, but not restricted to, the functional requirements. The service provider will have to facilitate the testing of all applications from MMRCL users during the operational acceptance.
- After the Operational Acceptance has occurred, the Service provider may give a notice to MMRCL's Project Manager requesting the issue of an Operational Acceptance Certificate.
- Once deficiencies have been addressed, the service provider shall notify MMRCL, and MMRCL, with the full cooperation of the 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 Service provider shall notify MMRCL of its request for Operational Acceptance Certification, MMRCL shall then issue to the service provider the Operational Acceptance Certification, or shall notify the Service provider of further deficiencies, or other reasons for the failure of the Operational Acceptance Test. The procedure set out in this clause shall be repeated, as necessary, until an Operational Acceptance Certificate is issued.
- If the System or Subsystem fails to pass the Operational Acceptance Test(s), then either:
  - MMRCL may consider terminating the Contract, or
  - If the failure to achieve Operational Acceptance within the specified time period is a result of the failure of MMRCL to fulfill its obligations under the Contract, then the

Service provider shall be deemed to have fulfilled its obligations with respect to the relevant technical and functional aspects of the Contract.

- Operational Acceptance will have to be performed for each phase.

## 4.17 Post Implementation Maintenance & Support

The 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 successful bidder has to provide post implementation support to maintain SLAs.

During the support period, if the successful bidder is unable to comply with the support terms, the bidder 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 3 months), during regular operations while only replication is taking place, in disaster scenario when DR is active and operational, and during switchover and switchback.

## 4.18 Helpdesk / Customer Support

- The service provider shall provide a centralized helpdesk/ customer care center telephone number/ E-mail/ fax number for attending user request/ complaints. The helpdesk/customer care center shall operate during working hours as per MMRCL for the support period. A detailed escalation plan shall have to be submitted before the commissioning of the services, consisting of not more than 4 tiers from helpdesk to Global/Country Service Manager.
- The service provider shall provide an incident tracking system via a web interface / mail / IVR, available in real-time which will issue a trouble ticket once a complaint is booked successfully. This trouble ticket system should be capable of generating monthly/quarterly/half yearly/yearly reports.
- The help desk service will serve as a single point of contact for all incident sand service requests at the Service Provider. The service will provide a Single Point of Contact (SPOC) and also escalation / closure of incidents for the IT/User departments whose infrastructure is hosted at the cloud site. The activities related to Cloud shall include the following:
  - Solution should comprise of a completely automated 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.
  - The solution provider shall ensure that if any tickets pertain to action from their end, these calls are fully responded by the professional team.

- Provide Help Desk facility during agreed service period window for reporting user department incidents / issues / problems with the IT infrastructure.
- Provide necessary channels for reporting issues to the help desk.
- 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 the SLAs.
- Creation of knowledge base on frequently asked questions to assist user departments in resolving basic issues themselves Track each incident / call to resolution
- Provide feedback to callers.
- Analyze the call statistics
- Creation of knowledge base on frequently asked questions to aid users. Any call logs and its associated resolution shall be stored in knowledge management database for future reference
- Escorting of MMRCL IT department executives to the server farm area (for any inspection etc.) will be done by helpdesk team
- Continuous monitoring of the c0-located (MMRCL owned) as well as cloud based IT infrastructure at the site to ensure availability as per agreed SLAs.
- Escalate the calls, to the appropriate levels, if necessary as per the escalation matrix agreed between the SI and the user department. The escalation matrix shall be developed by the SI in discussion with the SIA.
- 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

## 4.19 Server Monitoring, Administration

The activities shall include:

- Configuration of server parameters, operating systems administration and tuning.
- Operating system administration, including but not limited to management of users, processes, resource contention, preventive maintenance and management of updates & patches to ensure that the system is properly updated, with minimum or no downtime.
- The Service Provider shall support multiple users with a management portal.
- The Service Provider shall provide Billing / Invoice tracking through a web portal aggregated by user application and service at mutually agreed intervals based on components and services as listed in Financial Format.
- Service Provider should provide multi-factor authentication for accessing the cloud infrastructure and application.

- The Service Provider should provide Role Based Access Control to segregate users based on their roles and privileges.
- The Service Provider should provide the capability to log all operations being conducted on the infrastructure by any user.
- The Service Provider should provide ability to set up alerts and monitoring for different parameters to track health and usage of the infrastructure.
- Re-installation in the event of system crash/failures.
- Maintenance of a log of the performance monitoring of servers including but not limited to monitoring CPU, disk space, memory utilization, I/O utilization, etc.
- Event log analysis generated in all the sub systems including but not limited to servers, operating systems, applications, etc. Ensuring that the logs are backed up and truncated at regular intervals.
- Periodic health check of the systems (covering all cloud resources offered: IaaS and PaaS components etc.), troubleshooting problems, analyzing and implementing rectification measures.
- Alerts shall be provided by Cloud Service Provider to the concerned department / IT Department of the MMRCL if 70% of the allocated capacity of resources is being utilized.
- Ensuring the upkeep of existing systems that would be reused and also incorporate necessary changes for new applications if any during the tenure of the contract.
- Identification, diagnosis and resolution of problem areas pertaining to the MMRCL Cloud infrastructure and application and maintenance of assured SLA levels.
- Prepare, Design, implement and maintain standard operating procedures for maintenance of the Cloud infrastructure based on the MMRCL's policies.

## 4.20 Backup and Restore Services

The Service Provider shall provide backup solution (LTO6 tapes, or Disk-based backup in conjunction with Tape based backup), policies and procedures that is suitable to MMRCL environment, in consultation with IT Department and FMS Vendor of MMRCL. The activities shall include, but not limited to:

- Backup of operating system, Virtual Machines and application as per stipulated policies at the MMRCL.
- Monitoring and enhancement of the performance of scheduled backups, schedule regular testing of backups and ensure adherence to related retention policies.
- Real-time monitoring, log maintenance and reporting of backup status on a regular basis. Prompt problem resolution in case of failures in the backup processes
- MMRCL will review backup and restoration mechanism from time to time, in line with advancement in the technologies and the backup/restoration mechanism would be

finalized in consultation with the service provider. This will have no commercial bearings.

## 4.21 MIS Reports

Service Provider shall submit the reports on a regular basis in a mutually decided format. The Service Provider shall workout the formats for the MIS reports and get these approved by the MMRCL within a month of being awarded the contract. The following is only an indicative list of MIS reports that may be submitted to the MMRCL:

- Daily reports
  - Summary of issues / complaints logged at the Help Desk
  - Summary of resolved, unresolved and escalated issues / complaints
  - Summary of resolved, unresolved and escalated issues / complaints to vendors.
  - Log of backup and restoration undertaken.
- 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 on in
- Monthly reports
  - Component wise server as well as Virtual machines availability and
  - resource utilization
  - Consolidated SLA / (non)- conformance report.
  - Summary of component wise uptime.
  - Log of preventive / scheduled maintenance undertaken
  - Log of break-fix maintenance undertaken
  - All relevant reports required for calculation of SLAs
- 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 the MMRCL.
- The service provider will also provide any other report requested by the MMRCL or any other agency approved and authorized by MMRCL.

## 4.22 Input to Periodic Disaster Recovery Plan Update

The service provider shall be responsible providing input for

- Devising and documenting the DR policy discussed and approved by MMRCL.
- Providing data storage mechanism with from the Go-Live date till the date of contract expiry for the purpose of compliance and audit.

## 4.23 Hardware Upgrades & Software Updates

Any required version/Software /Hardware/ License upgrades, patch management etc. at the Cloud Site will be supported by the solution provider for the entire contract period at no extra cost to MMRCL.

## 4.24 Security Audits

The service provider shall conduct vulnerability and penetration test (from a third party testing agency which may be CERT-IN empanelled) on the proposed Cloud solution in every 6 months and reports should be shared. The service provider needs to update the system in response to any adverse findings in the report, without any additional cost to MMRCL. MMRCL may also depute auditors to conduct security check/ vulnerability test/penetration test.

## 4.25 Coordination, Cooperation and Support to FMS vendor of MMRCL

- During all phases of the project, the Implementation Agency shall have coordination and full cooperation with the FMS server provider of MMRCL. Since the project infrastructure has to be fully integrated with the MMRCL IT Environment, the Implementation agency will require support and from FMS and vice versa.
- MMRCL shall ensure that FMS service provider shall cooperate with the implementation agency and provide all necessary support, configuration settings, access to requisite and necessary IT assets.
- The service provider shall support the FMS team of MMRCL for the following activities:
  - Co-ordinating issues for timely resolution.
  - Knowledge Transfer of all activities performed by the service provider as part of installation, configuration, setup, operate and maintain.

## 4.26 Provisioning Cloud services for additional quantities at same rate

- Based on future requirements, MMRCL is likely to purchase additional quantities of cloud service covered in this Tender requirement.
- The rates offered cloud services must be valid for entire contract/project duration. No variation in these quoted rates shall be allowed during this period.

- MMRCL will have liberty to order additional cloud service items, at the rates offered in the commercial bid.

## 4.27 Service Level Agreement (SLAs)

- Cloud "Service Level Objective" (SLO) means the target for a given attribute of a cloud service that can be expressed quantitatively or qualitatively.
- Cloud SLAs means documented agreement between the service provider and the Department that identifies services and cloud service level objectives (SLOs).
- Response time is the time interval between a cloud service customer initiated event (e.g., logging of the request) and a cloud service provider initiated event in response to that stimulus.
- "Scheduled Maintenance Time" shall mean the time that the System is not in service due to a scheduled activity. Scheduled maintenance time is planned downtime with the prior permission of the Department, during non-business hours. The Scheduled Maintenance time <<within 10 hours a month>> as agreed shall not be considered for SLA Calculation.
- "Scheduled operation time" means the scheduled operating hours of the System for the month. All scheduled maintenance time on the system would be deducted from the total operation time for the month to give the scheduled operation time.
- "Availability" means the time for which the cloud services and facilities are available for conducting operations on the Department system.
- Availability is defined as:
- {(Scheduled Operation Time – System Downtime) / (Scheduled Operation Time)} * 100%
- "Incident" refers to any event/issue that affects the normal functioning of the services / infrastructure, reported by the cloud consumer to the Cloud Service provider (CSP) can be termed as an Incident.
- "Incident" refers to any event / abnormalities in the functioning of the IT Infrastructure solution and services that may lead to disruption in normal operations.
  i. "Helpdesk Support" shall mean the 24x7x365 centre which shall handle Fault reporting, Trouble Ticketing and related enquiries during this contract.
  ii. "Response Time" shall mean the time incident is reported to the help desk and an engineer is assigned for the call.
- "Resolution Time" shall mean the time taken (after the incident has been reported at the helpdesk), in resolving (diagnosing, troubleshooting and fixing) or escalating (to the second level) getting the confirmatory details about the same from the Agency and conveying the same to the end user), the services related troubles during the first level escalation.
- The resolution time shall vary based on the severity of the incident reported at the help desk. The severity would be as follows:

  - Critical : Critical/Central IT Infrastructure solution down impacting critical business functions or multiple modules/functions down impacting users on daily operations or any module/functionality deemed as highly critical by MMRC .
  - High: IT Infrastructure solution down impacting critical business functions or multiple modules/functions down impacting users on daily operations or any module /functionality deemed as highly critical by MMRC.
  - Medium: One module/functionality down impacting critical business functions having major impact on daily operations.
  - Low: Loss of business functionality for less than 10 users impacting day to day operations or minor functionality down impacting less than 10 users.
- Commencement of SLA: The SLA shall commence from implementation period itself for adherence to the implementation plan. The penalty will be deducted from the payment milestone during the implementation period. During the O & M period, the penalty will be deducted from the quarterly payments.

### SLA Review Process and Penalty

a. Either MMRC or bidder may raise an issue by documenting the business or technical problem, which presents a reasonably objective summary of both points of view and identifies specific points of disagreement with possible solutions.

b. A meeting or conference call will be conducted to resolve the issue in a timely manner. The documented issues will be distributed to the participants at least 24 hours prior to the discussion if the issue is not an emergency requiring immediate attention.

c. The MMRC and the bidder shall develop an interim solution, if required, and subsequently the permanent solution for the problem at hand. The bidder will then communicate the resolution to all interested parties.

d. In case the issue is still unresolved, the arbitration procedures described in the Terms & Conditions section will be applicable.

e. Three consecutive quarterly deductions of more than 10% of the applicable fee on account of any reasons will be deemed to be an event of default and likely termination.

f. If the penalty reaches 10% of the total contract value, MMRC may invoke termination clause.

For the Departments to ensure that the Cloud Service Providers adhere to the Service Level Agreements, this section describes the Penalties which may be imposed on CSPs. In case these service levels cannot be achieved at service levels defined in the agreement, the departments shall invoke the performance related penalties. Payments to the Service Provider to be linked to the compliance with the SLA metrics laid down below. To illustrate calculation of penalties, an indicative example is provided below.

a. The penalty in percentage of the <<Periodic Payment>> is indicated against each SLA parameter in the table.
    i. For ex: For SLA1 if the penalty to be levied is 7% then 7% of the <<Periodic Payment >>) is deducted from the total of the <<periodic> bill and the balance paid to the SP.
    ii. If the penalties are to be levied in more than one SLA then the total applicable penalties are calculated and deducted from the total of the <<periodic> bill and the balance paid to the SP.

    For ex: SLA1 =7% of the <<Periodic Payment>>, SLA12=10% of the <<Periodic Payment >>, SLA19=2% of the <<Periodic Payment>> then,

    Amount to be paid = Total <<periodic > bill – {(19% of the <<Periodic Payment>>)}

**Periodic Payment – Quarterly Payment**

**T- Issuance of LOA**

| # | Service Level Objective | Measurement Methodology / | Target/Service Level | Penalty |
|---|---|---|---|---|
| **Service Levels for CSP** | | | | |
| **Implementation related SLAs** | | | | |
| 1. | Network / Communication Links<br>Design, Configuration, Testing, Installation and Setup of ILL Connectivity as required. | Within 1 month from the issuance of LOA (T) | This will be calculated on basis of days of delay | a) Within one month from T - Nil<br>b) For every 7 days of delay 10% of QP.<br>The Bidder would be required to provide proper justification for the delay. If MMRC feels that the justification provided by the Bidder is not credible, the contract may be terminated. Penalty shall be paid in Demand Draft payable to MMRC. Failure to pay penalty may result in penalty amount deducted |

| # | Service Level Objective | Measurement Methodology / | Target/Service Level | Penalty |
|---|---|---|---|---|
| | | | | from Security Deposit. |
| 2. | Cloud Solution Implementation and Migration<br>Provisioning of the cloud resources and Migration of the application on new Cloud Environment | Within two months from T | This will be calculated on basis of days of delay | a) Within two months from T - Nil<br>b) For every 7 days of delay 10% of QP.<br>The Bidder would be required to provide proper justification for the delay. If MMRC feels that the justification provided by the Bidder is not credible, the contract may be terminated.<br>Penalty shall paid in Demand Draft payable to MMRC. Failure to pay penalty may result in penalty amount deducted from Security Deposit. |
| 3. | Operational Acceptance and Go-Live<br>User Acceptance Test Report, Operational Acceptance Report, Go-Live report | Within three months from T | This will be calculated on basis of days of delay | a) Within three months from T- Nil<br>b) For every 7 days of delay 10% of QP.<br>If the Bidder fails to pass the operational acceptance even after 3 unsuccessful attempts, MMRC |

| # | Service Level Objective | Measurement Methodology / | Target/Service Level | Penalty |
|---|---|---|---|---|
| | | | | may consider terminating the contract and the PBG will be forfeited.<br>Penalty shall paid in Demand Draft payable to MMRC. Failure to pay penalty may result in penalty amount deducted from Security Deposit |
| **Availability/Uptime** | | | | |
| 1. | Availability/Uptime of cloud services Resources for Production environment (VMs, Storage, OS, VLB, Security Components) | Availability (as per the definition in the SLA) will be measured for each of the underlying components (e.g., VM, Storage, OS, VLB, Security Components) provisioned in the cloud. Measured with the help of SLA reports provided by CSP. | Availability for each of the provisioned resources: >=99.5%<br>Monitoring shall be on monthly basis. | Default on any one or more of the provisioned resource will attract penalty as indicated below.<br><99.5% & >=99% ( 10% of the <<Periodic Payment>>)<br>< 99% (30% of the << Periodic Payment>>) |
| 2. | Availability of Critical Services (e.g., Register Support Request or Incident; Provisioning / De-Provisioning; User Activation / De-Activation; User Profile Management; Access Utilization Monitoring Reports) over User / Admin Portal and APIs (where applicable) | Availability (as per the definition in the SLA) will be measured for each of the critical services over both the User / Admin Portal and APIs (where applicable) | Availability for each of the critical services over both the User / Admin Portal and APIs (where applicable) >= 99.5%.<br>Monitoring shall be on monthly basis. | Default on any one or more of the services on either of the portal or APIs will attract penalty as indicated below.<br><99.5% and >= 99% ( 10% of the <<Periodic Payment>>)<br><99% ( 20% of the <<Periodic Payment>>) |

| # | Service Level Objective | Measurement Methodology / | Target/Service Level | Penalty |
|---|---|---|---|---|
| 3. | Availability of the network links at DC and DR (links at DC / DRC, DC-DRC link ) | Availability (as per the definition in the SLA) will be measured for each of the network links provisioned in the cloud. | Availability for each of the network links: >= 99.5%.<br>Monitoring shall be on monthly basis. | Default on any one or more of the provisioned network links will attract penalty as indicated below.<br><99.5% & >=99% ( 10% of the <<Periodic Payment>>) < 99% (30% of the <<Periodic Payment>>) |
| 4. | Availability of Regular Reports | | 15 working days from the end of the quarter.<br>If STQC issues a certificate based on the audit then this SLA is not required. | 5% of <<periodic Payment>> |
| **Support Channels - Incident and Helpdesk** | | | | |
| 1. | Response Time | Average Time taken to acknowledge and respond, once a ticket/incident is logged through one of the agreed channels. This is calculated for all tickets/incidents reported within the reporting month. | 95% within 15 minutes | <95% & >=90% ( 5% of the <<Periodic Payment>>) < 90% & >= 85% ( 7% of the <<Periodic Payment>>) < 85% & >= 80% ( 9% of the <<Periodic Payment>>) |
| 2. | Time to Resolve - Severity 1 | Time taken to resolve the reported ticket/incident from the time of logging. | For Severity 1, 98% of the incidents should be resolved within 30 minutes of problem reporting | <98% & >=90% ( 5% of the <<Periodic Payment>>) < 90% & >= 85% ( 10% of the <<Periodic Payment>>) < 85% & >= 80% ( 20% of the |

| # | Service Level Objective | Measurement Methodology / | Target/Service Level | Penalty |
|---|---|---|---|---|
| | | | | <<Periodic Payment>>) |
| 3. | Time to Resolve - Severity 2,3 | Time taken to resolve the reported ticket/incident from the time of logging. | 95% of Severity 2 within 4 hours of problem reporting AND 95% of Severity 3 within 16 hours of problem reporting | <95% & >=90% ( 2% of the <<Periodic Payment>>) < 90% & >= 85% ( 4% of the <<Periodic Payment>>) < 85% & >= 80% ( 6% of the <<Periodic Payment>>) |
| **Security Incident and Management Reporting** | | | | |
| 1. | Percentage of timely incident report | Measured as a percentage by the number of defined incidents reported within a predefined time (1 hour) limit after discovery, over the total number of defined incidents to the cloud service which are reported within a predefined period (i.e. month). Incident Response - CSP shall assess and acknowledge the defined incidents within 1 hour after discovery. | 95% within 1 hour | <95% & >=90% ( 5% of the <<Periodic Payment>>) < 90% & >= 85% (10% of the <<Periodic Payment>>) < 85% & >= 80% ( 15% of the <<Periodic Payment>>) |
| 2. | Percentage of timely incident resolutions | Measured as a percentage of defined incidents against the cloud service that are resolved within a predefined time limit (month) over the total number of defined incidents to the cloud service within a | 95% to be resolved within 1 hour | <95% & >=90% ( 5% of the <<Periodic Payment>>) < 90% & >= 85% (10% of the <<Periodic Payment>>) < 85% & >= 80% ( 15% of the |

| # | Service Level Objective | Measurement Methodology / | Target/Service Level | Penalty |
|---|---|---|---|---|
| | | predefined period. (Month). Measured from Incident Reports | | <<Periodic Payment>>) |
| **Vulnerability Management** | | | | |
| 1. | Percentage of timely vulnerability corrections | The number of vulnerability corrections performed by the cloud service provider - Measured as a percentage by the number of vulnerability corrections performed within a predefined time limit, over the total number of vulnerability corrections to the cloud service which are reported within a predefined period (i.e. month). • High Severity Vulnerabilities – 30 days - Maintain 99.95% service level • Medium Severity Vulnerabilities – 90 days - Maintain 99.95% service level | 99.95% | >=99% to <99.95% [ 10% of Periodic Payment] >=98% to <99% [ 20% of Periodic Payment] <98% [ 30% of Periodic Payment] |
| 2. | Percentage of timely vulnerability reports | Measured as a percentage by the number of vulnerability reports within a predefined time limit, over the total number of vulnerability reports to the cloud service which are reported within a predefined period (i.e. month). | 99.95% | >=99% to <99.95% [ 10% of Periodic Payment] >=98% to <99% [ 20% of Periodic Payment] <98% [ 30% of Periodic Payment] |
| 3. | Security breach including Data Theft /Loss/Corruption | Any incident where in system compromised or any case wherein data theft occurs (including internal incidents) | No breach | For each breach/data theft, penalty will be levied as per following criteria. Any security incident detected |

| # | Service Level Objective | Measurement Methodology / | Target/Service Level | Penalty |
|---|---|---|---|---|
| | | | | INR 5 Lakhs. This penalty is applicable per incident. These penalties will not be part of overall SLA penalties cap per month. In case of serious breach of security wherein the data is stolen or corrupted, MMRC reserves the right to terminate the contract. |
| 4. | Availability of SLA reports covering all parameters required for SLA monitoring within the defined time | | 3 working days from the end of the month | 5% of <<periodic Payment>> |
| **Service levels for MSP/SI** | | | | |
| 1. | Recovery Time Objective (RTO) | Measured during the regular planned or unplanned (outage) changeover from DC to DR or vice versa. | RTO <= 2 hours> | 10% of <<Periodic Payment>> per every additional 2 (two) hours of downtime. |
| 2. | Recovery Point Objective (RPO ) | Measured during the regular planned or unplanned (outage) changeover from DC to DR or vice versa. | RPO <= 30 mins | 10% of <<Periodic Payment>> per every additional 30 mins of downtime |
| 3. | Availability of Root Cause Analysis (RCA) reports for Severity 1 & 2 | | Average within 5 Working days | 5% of <<periodic Payment>> |

The severity would be defined as follows:

| 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.<br>No access to Storage, software or application |
| Severity 2 | Loss of performance resulting in users (includes public users) being unable to perform their normal activities as essential functions and critical programs are partially available or severely restricted. Inconvenient 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. | |

## 4.28 Exit Management

1. Service Provider (SP) shall decommission and withdraw all hardware and software components after the completion of the contract period and formally close the project. This process will be initiated 6 months before the ending of the project contract. In order to align both the parties on transition modalities, Service Provider will submit a detailed Exit Management Plan before 6 months of the ending date of the contract. Exit Management Plan will include following but limited to:
   a. Detailed inventory of all the assets, IT Infrastructure, its location, condition, licenses, documents, manuals, etc. created under the Project.
   b. Method of Transition including roles and responsibilities of both the parties to handover and takeover the charge of project regular activities and support system.
   c. Proposal for necessary setup or institution structure required at MMRC level to effectively maintain the project after contract ending.

d. Training and handholding of MMRC Staff or designated officers for maintenance of project after contract ending.

2. MMRC will approve this plan after necessary consultation and start preparation for transition.

# 5. General Conditions of Contract

## 5.1 General Guidelines

1. The system of recording, measurements and payments will be based on the MMRC in vogue.
2. It is presumed that the contractor has gone carefully the standard and special specification of the individual items and studied the site condition before arriving at the percentage above / below the estimated rates quoted by him.
3. Special provisions in the detailed specifications or wording of any item shall give precedence over the corresponding contract provisions, if any. In case of any contradictions in the specifications, the interpretation and decision of the IT in-charge shall be final and binding.
4. If the bidder has any doubts, whatsoever, as to the contents of the contract he is deemed to have in good time i.e. before submitting his tender, get his doubts clarified authoritatively from the Contact Person in writing. Once the tender is submitted by bidder, the matter will be decided according to the tender stipulations.
5. All the time of work in Schedule-B of the tender are completed items of work and no extra claims shall be accepted as regards specifications, infrastructure, all taxes (Sales Tax, GST, etc.), royalties, and any other applicable taxes / charges etc.

## 5.2 Interpretation

In this Contract unless a contrary intention is evident:

1. the clause headings are for convenient reference only and do not form part of this Contract;
2. unless otherwise specified a reference to a clause number is a reference to all of its sub-clauses;
3. unless otherwise specified a reference to a clause, sub-clause or section is a reference to a clause, sub- clause or section of this Contract including any amendments or modifications to the same from time to time;
4. a word in the singular includes the plural and a word in the plural includes the singular;
5. a word importing a gender includes any other gender;
6. a reference to a person includes a partnership and a body corporate;
7. a reference to legislation includes legislation repealing, replacing or amending that legislation;
8. Where a word or phrase is given a particular meaning it includes the appropriate grammatical forms of that word or phrase which have corresponding meanings.
9. In the event of an inconsistency between the terms of this Contract and the Tender and the Bid, the terms hereof shall prevail.

## 5.3 Key Performance Measurements

1. Unless specified by the Purchaser to the contrary, the Service Provider shall implement the infrastructure, perform the Services and carry out the Scope of Work in accordance with the terms of this Contract, Scope of Work and the Service Specifications as laid down under Service Level Agreement.
2. If the Contract / Service Specification include more than one document, then unless the Purchaser specifies to the contrary, the later in time shall prevail over a document of earlier date to the extent of any inconsistency.
3. The Purchaser reserves the right to amend any of the terms and conditions in relation to the Contract / Services and may issue any such directions which are not necessarily stipulated therein if it deems necessary for the fulfilment of the scope of work.

## 5.4 Commencement & Progress

The Service Provider shall commence the performance of its obligations in a manner as specified in the Scope of Work.

1. The Service Provider shall proceed to carry out the activities / services with diligence and expedition in accordance with any stipulation as to the time, manner, mode, and method of execution contained in this Contract.
2. The Service Provider shall be responsible for and shall ensure that all activities / services are performed in accordance with the Contract, Scope of Work and that the Service Provider's Team complies with such specifications and all other standards, terms and other stipulations/conditions set out hereunder.
3. The Service Provider shall perform the activities / services and carry out its obligations under the Contract with due diligence, efficiency and economy, in accordance with generally accepted techniques and practices used in the industry and with professional engineering and consulting standards recognized by international professional bodies and shall observe sound management, engineering and security practices. It shall employ appropriate advanced technology and engineering practices and safe and effective equipment, machinery, material and methods. The Service Provider shall always act, in respect of any matter relating to this Contract, as faithful advisors to the Purchaser and shall, at all times, support and safeguard the Purchaser's legitimate interests in any dealings with Third parties.

## 5.5 Trademarks, Publicity

Neither Party may use the trademarks of the other Party without the prior written consent of the other Party. Neither Party shall publish nor did permitted to be publish either along with or in conjunction with any other person any press release, information, article, photograph, illustration or any other material of whatever kind relating to this Agreement, the SLA or the business of the Parties without prior reference to and approval in writing from the other Party.

## 5.6 Ethics

Service Provider represents, warrants and covenants that it has given no commitments, payments, gifts, kickbacks, lavish or expensive entertainment, or other things of value to any employee or Board, or its nominated agencies in connection with this agreement and acknowledges that the giving of any such payment, gifts, entertainment, or other things of value is strictly in violation of Purchaser standard policies and may result in cancellation of this Agreement.

## 5.7 Purchaser's Obligations

1. Purchaser nominated representative shall act as the nodal point for implementation of the contract and for issuing necessary instructions, approvals, commissioning, acceptance certificates, payments etc. to the Service Provider.
2. Purchaser shall ensure that timely approval is provided to the Service Provider as and when required, which may include approval of project plans, implementation methodology, design documents, specifications, or any other document necessary in fulfilment of this contract.
3. The Purchaser's Representative shall interface with the Service Provider, to provide the required information, clarifications, and to resolve any issues as may arise during the execution of the Contract. Purchaser shall provide adequate cooperation in providing details, coordinating and obtaining of approvals from various governmental agencies, in cases, where the intervention of the Purchaser is proper and necessary.
4. Purchaser may provide on Service Provider's request, particulars/information/ or documentation that may be required by the Service Provider for proper planning and execution of work and for providing services covered under this contract and for which the Service Provider may have to coordinate with respective vendors.
5. Purchaser may provide to the Service Provider, sitting space and basic infrastructure at the Board's office location.

## 5.8 Events of default by the Service Provider

The failure on the part of the Service Provider to perform any of its obligations or comply with any of the terms of this Contract shall constitute an Event of Default on the part of the Service Provider. The events of default as mentioned above may include inter-alia the following:

1. The Service Provider's Team has failed to perform any instructions or directives issued by the Purchaser which it deems proper and necessary to execute the scope of work or provide services under the Contract, or.
2. The Service Provider's Team has failed to confirm / adhere to any of the key performance indicators as laid down in the Key Performance Measures / Service Level Agreements, or if the Service Provider has fallen short of matching such standards / benchmarks / targets as the Purchaser may have designated with respect to the system or any goods,

task or service, necessary for the execution of the scope of work and performance of services under this Contract. The above mentioned failure on the part of the Service Provider may be in terms of failure to adhere to performance, quality, timelines, specifications, requirements or any other criteria as defined by the Purchaser;

3. The Service Provider has failed to remedy a defect or failure to perform its obligations in accordance with the specifications issued by the Purchaser, despite being served with a default notice which laid down the specific deviance on the part of the Service Provider's Team to comply with any stipulations or standards as laid down by the Purchaser; or
4. The Service Provider's Team has failed to adhere to any amended direction, instruction, modification or clarification as issued by the Purchaser during the term of this Contract and which the Purchaser deems proper and necessary for the execution of the scope of work under this Contract.
5. The Service Provider's Team has failed to demonstrate or sustain any representation or warranty made by it in this Contract, with respect to any of the terms of its Bid, the Tender and this Contract.
6. There is a proceeding for bankruptcy, insolvency, winding up or there is an appointment of receiver, liquidator, assignee, or similar official against or in relation to the Service Provider.
7. The Service Provider's Team has failed to comply with or is in breach or contravention of any applicable laws.
8. The Service Provider's team are involved in fraud/wilful misconduct.
9. Where there has been an occurrence of such defaults inter alia as stated above, the Purchaser shall issue a notice of default to the Service Provider, setting out specific defaults / deviances / omissions / non-compliances / non-performances and providing a notice of Sixty (60) days to enable such defaulting party to remedy the default committed.
10. Where despite the issuance of a default notice to the Service Provider by the Purchaser the Service Provider fails to remedy the default to the satisfaction of the Service Provider, the Purchaser may, where it deems fit, issue to the defaulting party another default notice or proceed to adopt such remedies as may be available to the Purchaser.

## 5.9 Consequences of Default

Where an Event of Default subsists or remains uncured the Purchaser shall be entitled to:

1. Impose any such obligations and conditions and issue any clarifications as may be necessary to inter alia ensure smooth continuation of project and the Services which the Service Provider shall be obliged to comply with which may include re-determination of the consideration payable to the Service Provider as agreed mutually by Purchaser and Service Provider or through a third party acceptable to both parties. The Service Provider shall in addition take all available steps to minimize loss resulting from such event of default.

2. Suspend all payments to the Service Provider under the Contract by a written notice of suspension to the Service Provider, provided that such notice of suspension:
    a. Shall specify the nature of the failure; and
    b. Shall request the Service Provider to remedy such failure within a specified period from the date of receipt of such notice of suspension by the Service Provider.

## 5.10 Audit, Access and Reporting

### 5.10.1 Purpose

1. This section details the audit, access and reporting rights of Purchaser and the respective obligations of Service Provider under the contractual terms of Project Implementation, Operation and SLA Management.
2. Purchaser shall engage a suitable, neutral and technically competent third party agency or agencies for conducting audit and certification, upon intimation by the Service Provider that the system implementation is complete.
3. The Service Provider being notified of any deviations from the agencies nominated by Purchaser regarding deviations from norms, standards or guidelines shall at the earliest instance, take all corrective measures required in least possible time.

### 5.10.2 Notice and Timing

1. 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 in accordance with such agreed timetable and shall not be required to give the Service Provider any further notice of carrying out such audits.
2. The Purchaser or its nominated agencies may conduct non-timetabled audits at its own discretion if they reasonably believe that such non-timetabled audits are necessary as a result of an act of fraud by the Service Provider, a security violation, or breach of confidentiality obligations by the Service Provider, provided that the requirement for such an audit is notified in writing to the 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. If the Service Provider considers that the non-timetabled audit was not appropriate, the matter shall be referred to the escalation procedure.
3. The frequency of audits shall be decided by the Purchaser
4. In addition to the above, there will be audits conducted by statutory bodies (e.g. CAG) as and when they are required to do it. Notwithstanding any condition given in the contract, the Service Provider will have to provide these statutory bodies access to all the facilities,

infrastructure, documents and artefacts of the Project as required by them and approved by purchaser, in writing.

5. The audit and access rights contained shall survive the termination or expiration of the Agreement.

### 5.10.3 Access

1. The Service Provider shall provide Purchaser access to documents, records and systems reasonably required for audit and shall provide all such persons with routine assistance in connection with the audits and inspections.
2. Purchaser shall have the right to copy and retain copies of any relevant records. The Service Provider shall co- operate with Purchaser in effecting the audits and providing necessary information.

### 5.10.4 Inspection Rights

1. Purchaser shall have the right to inspect data centre, data recovery centres, 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:
    a. The security, integrity and availability of all Project data processed, held or conveyed by the Service Provider on behalf of Project and documentation related thereto;
    b. That the actual level of performance of the services is the same as specified in the SLA;
    c. That the Service Provider has complied with the relevant technical standards, and has adequate internal controls in place; and
    d. The compliance of the Service Provider with any other obligation under the contract and SLA.

## 5.11 Data Ownership

All the data created as the part of the project would be owned by the purchaser. Successful Bidder shall take utmost care in maintaining security, confidentiality and backup of this data.

## 5.12 Other Conditions

### 5.12.1 Indemnity

The Service Provider shall indemnify the MMRC against the all actions, suits, claims, damages and demands brought or made against him in respect of anything done or omitted to be done by the Service Provider in the execution of or in the connection with the work of this contract and against loos or damage to the MMRC in consequences of any action or suit being brought against the contractor anything done or omitted to be done in execution of the work of this contract.

### 5.12.2 Corrupt or Fraudulent Practices:

1. The MMRCL requires that Bidders/Suppliers/Contractors under contracts, observe the highest standard of ethics during the procurement and execution of such contracts. In pursuance of this policy MMRCL.
2. Defines, for the purposes of this provision, the terms set forth below as follows:
3. "Corrupt practice" means the offering, giving, receiving or soliciting of anything of value to influence the action of a public official in the procurement process or in contract execution; and
4. "Fraudulent practice" means a misrepresentation of facts in order to influence a procurement process or the execution of a contract.
5. Will reject a proposal for award if it determines that the bidder recommended for award has engaged in corrupt or fraudulent practices in competing for the contract in question.
6. Will declare a firm ineligible, either indefinitely or for a stated period of time, to be awarded a contract if it any time determines that the firm has engaged in corrupt or fraudulent practices in competing for, or in executing, a contract.

### 5.12.3 Tendering Under Different Names:

1. Firms with common proprietor/partner or connected with one another either financially or as principal and agent or as master and servant or with proprietor/partners closely related to each as husband, wife, father, mother and minor son/daughter and brother/sister and minor brother/sister, shall not tender separately under different names for the same Contract.
2. If it is found that firms as described in (a) have tendered separately under different names for the same Contract, all such tender(s) shall stand rejected and tender deposit of each such firm /establishment shall be forfeited. In addition, such firms / establishments shall be liable, at the direction of the Managing Director, for further penal action including blacklisting.
3. If it is found that clearly related persons as in above have submitted separate tender/quotations under different names of firms/establishments but with common address for each establishment/firm, though they have different addresses, are managed or governed by the same person/persons jointly or severally, such Bidders shall be liable for action as in para above
4. If after the Award of Contract, it is found that the accepted tender violated for cancellation at any time during its currency in addition to penal action against the contractors as well as related firms / establishments.

### 5.12.4 Jurisdiction of Courts:

In case of any claim, dispute or difference rising in respect of the contract, the case of action there of shall be deemed to have arisen in Mumbai and all legal proceedings in respect of any such claim, dispute or difference shall be instituted in competent court in the city of Mumbai only. Employer, and includes collusive practice among bidders (prior to or after Tender submission) designed to establish Tender prices at artificial non-competitive levels and to deprive the employer of the benefits of free an open competition.

### 5.12.5 Import License:

The bidders shall have to make their own arrangements to secure import license and / or release of controlled or scares infrastructure if required by them for fulfilment of their contract. The Metropolitan Commissioner shall not be bound to give any assistance to the bidders in that behalf.

### 5.12.6 Safe Custody:

All the charges for safe custody and withdrawal of and for the collection of interest etc. on the proper deposit will be payable by the contractors.

### 5.12.7 Risk & Cost:

1. In case the contractor fails to deliver the quantity as stipulated in the delivery schedule, the Engineer in charge reserves right to procure same or similar material from alternate sources at risk, cost and responsibility of the contractor.
2. If it is observed that the Contractors carrying out the work fails to comply with instructions given by the authorities at the Superintending Engineer/ Executive Engineer's level during execution of work twice, the work will be carried out at the risk and cost of the contract & penal action will be taken against them. The above condition will be in addition to the relevant condition in General Condition of the Contract regarding cancellation of full or part of the work, finality of the decision of the disputes, differences or claims raised by the contractors relating to any matter arising out of the contract

### 5.12.8 Conflict of Interest

Applicant shall furnish an affirmative statement as to the absence of, actual or potential conflict of interest on the part of the Applicant or any prospective subcontractor due to prior, current, or proposed contracts, engagements, or affiliations with MMRC. Additionally, such disclosure shall address any and all potential elements (time frame for service delivery, resource, financial or other) that would adversely impact the ability of the Applicant to complete the requirements as given in the application document.

### 5.12.10 Confidentiality

1. The cloud service provider will be exposed, by virtue of the agreed activities as per the application document, to internal business information of MMRC and other Government

Departments. The service provider would be required to provide an undertaking that they will not use or pass to anybody the data/information derived from the project in any form. The service provider must safeguard the confidentiality of the MMRC's and Government Department's business information, applications and data. For this, service provider is required to sign Non-disclosure agreement with MMRC and Government Department (for the respective project).

2. Disclosure of any part of the afore mentioned information to parties not directly involved in providing the services requested, unless required to do so by the Court of Law within India or other Statutory Authorities of Indian Government, could result in premature termination of the Empanelment. The MMRC may apart from blacklisting the cloud service provider, initiate legal action against the cloud service provider for breach of trust. The cloud service provider shall also not make any news release, public announcements or any other reference on application document or empanelment agreement without obtaining prior written consent from the MMRC.
3. Service provider shall use reasonable care to protect confidential information from unauthorised disclosure and use.

### 5.12.11 Arbitration

If, due to unforeseen reasons, problems arise during the progress of the empanelment leading to disagreement between the MMRC and the service provider (or the Government Department and the service provider), both the MMRC (and the Government Department as the case may be) and the cloud service provider shall first try to resolve the same amicably by mutual consultation. If the parties fail to resolve the dispute by such mutual consultation within twenty-one days, then, depending on the position of the case, either MMRC (or the Government Department as the case may be) or the cloud service provider can give notice to the other party of its intention to commence arbitration and the applicable arbitration procedure will be as per Indian Arbitration and Conciliation Act,1996, and the venue of the arbitration will be New Delhi (or a city as determined by the Government Department in its MSA).

### 5.12.12 Governing law and Jurisdiction

This Empanelment Award and any dispute arising from it, whether contractual or non-contractual, will be governed by laws of India and subject to arbitration clause, be subject to the exclusive jurisdiction of the competent courts of Mumbai, India

### 5.12.13 Limitation of Liability

1. The liability of service provider (whether in contract, tort, negligence, strict liability in tort, by statute or otherwise) for any claim in any manner related to the Agreement, including the work, deliverables or Services covered by the Agreement, shall be the

payment of direct damages only which shall in no event in the aggregate exceed the total contract value (contract with the Government Department). The liability cap given under this Clause shall not be applicable to the indemnification obligations.

2. In no event shall either party be liable for any consequential, incidental, indirect, special or punitive damage, loss or expenses (including but not limited to business interruption, lost business, lost profits, or lost savings) even if it has been advised of their possible existence.
3. The allocations of liability in this clause represent the agreed and bargained-for understanding of the parties and compensation for the Services reflects such allocations. Each Party has a duty to mitigate the damages and any amounts payable under an indemnity that would otherwise be recoverable from the other Party pursuant to the Empanelment Award by taking appropriate and commercially reasonable actions to reduce or limit the amount of such damages or amounts.

### 5.12.14 Relationships

Nothing mentioned herein shall be construed as relationship of master and servant or of principal and agent as between the "MMRC" (or the Government Department) and the "Applicant". No partnership shall be constituted between MMRC (or the Government Department) and the Applicant by virtue of this empanelment nor shall either party have powers to make, vary or release their obligations on behalf of the other party or represent that by virtue of this or any other empanelment a partnership has been constituted, or that it has any such power. The Applicants shall be fully responsible for the services performed by them or on their behalf.

Neither party shall use the other parties name or any service or proprietary name, mark or logo of the other party for promotional purpose without first having obtained the other party's prior written approval.

### 5.12.15 Termination

1. MMRC may, without prejudice to any other remedy for breach of Contract, terminate this Contract in case of the occurrence of any of the events specified in paragraphs (1) through (11) of this GCC Clause 5.12.15.1. In such an occurrence, MMRC shall give a not less than 30 days' written notice of termination to the successful bidder.
2. If the successful bidder does not remedy a failure in the performance of its obligations under the Contract, within thirty (30) days after being notified or within any further period as MMRC may have subsequently approved in writing.
3. If the successful bidder becomes insolvent or goes into liquidation, or receivership whether compulsory or voluntary.
4. If the successful bidder, in the judgment of MMRC has engaged in corrupt or fraudulent practices in competing for or in executing the Contract.

5. If, as the result of Force Majeure, the successful bidder is unable to perform a material portion of the Services for a period of not less than 60 days.
6. If the successful bidder submits to the MMRC a false statement which has a material effect on the rights, obligations or interests of MMRC.
7. If the successful bidder places itself in a position of conflict of interest or fails to disclose promptly any conflict of interest to MMRC.
8. If the successful bidder fails to provide the quality services as envisaged under this Contract, MMRC may make judgment regarding the poor quality of services, the reasons for which shall be recorded in writing. MMRC may decide to give one chance to the successful Bidder to improve the quality of the services.
9. If the successful bidder fails to comply with any final decision reached as a result of arbitration proceedings.
10. In the event MMRC terminates the Contract in whole or in part, pursuant to GCC Clause 5.12.15.1, MMRC may procure, upon such terms and in such manner as it deems appropriate, services similar to those undelivered or not performed, and the successful bidder shall be liable to MMRC for any additional costs for such similar services. However, the successful bidder shall continue performance of the Contract to the extent not terminated.
11. MMRC shall not be liable for any payment in case of termination.

### 5.12.16 Assignment

The successful Bidder shall not assign, in whole or in part, their rights and obligations under this Contract to any third party, except with prior written consent of the other party."

### 5.12.17 Force Majure

1. Force Majeure shall not include any events caused due to acts/omissions of such Party or result from a breach/contravention of any of the terms of the Contract, Bid and/or the Tender. It shall also not include any default on the part of a Party due to its negligence or failure to implement the stipulated/proposed precautions, as were required to be taken under the Contract.
2. The failure or occurrence of a delay in performance of any of the obligations of either party shall constitute a Force Majeure event only where such failure or delay could not have reasonably been foreseen, or where despite the presence of adequate and stipulated safeguards the failure to perform obligations has occurred. In such an event, the affected party shall inform the other party in writing within five days of the occurrence of such event. The Purchaser will make the payments due for Services rendered till the occurrence of Force Majeure. However, any failure or lapse on the part of the Service Provider's Team in performing any obligation as is necessary and proper, to negate the damage due to projected Force Majeure events or to mitigate the damage that may be caused due to the abovementioned events or the failure to provide adequate disaster

management/recovery or any failure in setting up a contingency mechanism would not constitute force majeure, as set out above.

3. In case of a Force Majeure, all Parties will endeavour to agree on an alternate mode of performance in order to ensure the continuity of service and implementation of the obligations of a party under the Contract and to minimize any adverse consequences of Force Majeure.
4. The Service Provider shall not be liable for forfeiture of its performance security, liquidated damages or termination for default, if and to the extent that it's delay in performance or other failure to perform its obligations under the contract is the result of an event of force Majeure.
5. For purposes of this Clause, "Force Majeure" means an event beyond the control of the Vendor and not involving the Service Provider's fault or negligence and not foreseeable.
6. Such events may include, but are not limited to, Acts of God or of public enemy, acts of Government of India in their sovereign capacity, acts of war, acts of terrorism, either in fires, floods, strikes, lock-outs and freight embargoes.
7. If a Force Majeure situation arises, the Vendor shall promptly notify the Board in writing of such conditions and the cause thereof within twenty calendar days.
8. Unless otherwise directed by the Board in writing, the Vendor shall continue to perform its obligations under the Contract as far as it is reasonably practical, and shall seek all reasonable alternative means for performance not prevented by the Force Majeure event. In such a case, the time for performance shall be extended by a period(s) not less than the duration of such delay.
9. If the duration of delay continues beyond a period of three months, Board and the Service Provider shall hold consultations with each other in an endeavor to find a solution to the problem. Notwithstanding above, the decision of the MMRC, shall be final and binding on the Service Provider.

### 5.12.18 Non-Fulfilment of Conditions Precedent

1. In the event that any of the Conditions Precedent relating to Service Provider has not been fulfilled, as per the Implementation Schedule and the same has not been waived by Purchaser fully or partially, this Agreement shall cease to have any effect as of that date.
2. In the event that the Agreement fails to come into effect on account of nonfulfillment of the Service Provider's Conditions Precedent with regards to implementation schedule, Purchaser shall not be liable in any manner whatsoever to the Service Provider and Purchaser shall forthwith invoke the Performance Security Deposit (Bank Guarantee) and forfeit the guaranteed amount.
3. In the event that vacant possession of any of the Project facilities and/or Project Data has been delivered to the Service Provider prior to the fulfilment in full of the Conditions Precedent, upon the termination of this Agreement such Project facilities and Project data shall immediately revert to purchaser free and clear from any encumbrances or claims.

4. Instead of terminating this Agreement as stated above, the Parties may mutually agree in writing to extend the time for fulfilling the Conditions Precedent and the Term of this Agreement. It is further clarified that any such extension of time shall be subject to imposition of penalties on Service Provider linked to the delay in fulfilling the Conditions Precedent.

### 5.12.19 Governance Schedule

1. The Service Provider shall document the agreed structures in a procedural manual under the guidance and supervision of purchaser.
2. The agenda for each meeting of the Steering Committee and Project Operations Committee shall be set to reflect the discussion items related to the scope of work and additional items may be added either with the agreement of the Parties or at the request of either Party.
3. Copies of the agenda for meetings of the Steering Committee and Project Operations Committee, along with relevant pre-reading material, shall be distributed.
4. All meetings and proceedings will be documented; such documents to be distributed to both Parties and copies shall be kept as a record. All actions, responsibilities and accountabilities arising out of any meeting shall be tracked and managed.
5. Administrative decisions taken by MMRC, shall be binding on Service Provider.
6. The Parties shall ensure as far as reasonably practicable that the Steering Committee and Project Operations Committee shall resolve the issues and resolve the objectives placed before them and members representing that Party are empowered to make relevant decisions or have easy access to empowered individuals for decisions to be made to achieve this.
7. The Parties will proceed in good faith so that the Steering Committee and Project Operations Committee shall resolve the issues and smoothen the performance of the Project.
8. The parties agree to attempt to resolve all disputes arising under the Agreement, equitably and in good faith. To this end, the parties agree to provide frank, candid and timely disclosure of all relevant facts, information and documents to facilitate discussions between them/their representatives or senior officers.

# 6. Guidelines for Technical Proposal

## 6.1 Technical Proposal Bid Cover Letter

(To be submitted on the Letterhead of the responding firm)

Date: dd/mm/yyyy

To

Executive Director (Electrical)
MMRC,
Bandra - Kurla Complex
Bandra (East)
Mumbai—400 051

**Sub:** Selection of Bidder for the Project "for Hiring of "Cloud based Disaster Recovery services" from Managed Service Provider at Mumbai Metro Rail Corporation (MMRC)"

**Ref: RFP Notification number - MMRC/IT/RFP DC-DR/71**

Dear Sir,

Having examined the RFP, the receipt of which is hereby duly acknowledged, we, the undersigned, offer to provide the professional services as required and outlined in the RFP for **"Hiring of "Cloud based Disaster Recovery services" from Managed Service Provider at Mumbai Metro Rail Corporation (MMRC)** "

We attach hereto the technical response as required by the RFP, which constitutes our proposal. We undertake, if our proposal is accepted, to adhere to the implementation plan (Project schedule) for providing Professional Services in **"For Hiring of "Cloud based Disaster Recovery services" from Managed Service Provider at Mumbai Metro Rail Corporation (MMRC)** ", put forward in RFP or such adjusted plan as may subsequently be mutually agreed between us and MMRC or its appointed representatives.

If our proposal is accepted, we will obtain a Performance Security Deposit (Bank Guarantee) issued by a nationalized bank in India, for a sum of equivalent to 10% of the contract value for the due performance of the contract.

We agree for unconditional acceptance of all the terms and conditions set out in the RFP document and also agree to abide by this tender response for a period of 180 days from the date of submission of Bid and it shall remain binding upon us with full force and virtue, until within this period a formal contract is prepared and executed, this tender response, together with your written acceptance thereof in your notification of award, shall constitute a binding contract between us and MMRC.

We confirm that the information contained in this proposal or any part thereof, including its exhibits, schedules, and other documents and instruments delivered or to be delivered to MMRC is true, accurate, and complete. This proposal includes all information necessary to ensure that the statements therein do not in whole or in part mislead MMRC as to any material fact.

We agree that you are not bound to accept any tender response you may receive. We also agree that you reserve the right in absolute sense to reject all or any of the products/ services specified in the tender response.

It is hereby confirmed that I/We are entitled to act on behalf of our company/ corporation/ firm/ organization and empowered to sign this document as well as such other documents, which may be required in this connection.

Date:
(Signature)
(Name)
(In the capacity of)
[Seal / Stamp of bidder]
Witness Signature:
Witness Name:
Witness Address:

----------------------------------------------------------------------------------------------------------------

## CERTIFICATE AS TO AUTHORISED SIGNATORIES

I________________________, the Company Secretary of _______________, certify that________________________________ who signed the above Bid is authorized to do so and bind the company by authority of its board/ governing body.

Date:
Signature:
(Company Seal) (Name)

## 6.2 Format to share Bidder's and Bidding Firms Particulars

The Table below provides the format in which general information about the bidder must be furnished.

| S No | Information | Details |
|---|---|---|
| 1. | Name of Bidding firm: | |
| 2. | Address and contact details of Bidding firm: | |
| 3. | Firm Registration Number and Year of Registration | |
| 4. | Web Site Address | |
| 5. | Status of Company (Public Ltd., Pvt. Ltd., etc.) | |
| 6. | Company's Permanent Account Number (PAN) & GST | |
| 7. | Company's Revenue for the last 3 years (Year wise) | |
| 8. | Name, Designation and Address of the contact person to whom all references shall be made regarding this RFP: | |
| 9. | Telephone number of contact person: | |
| 10. | Mobile number of contact person: | |
| 11. | Fax number of contact person: | |
| 12. | E-mail address of contact person: | |
| 13. | Sub-Contracting Company Name (if any) | |
| 14. | Mailing Address and contact details of Bidding firm: | |
| 15. | Web Site Address | |
| 16. | Firm Registration Number and Year of Registration | |
| 17. | Status of Company (Public Ltd., Pvt. Ltd., etc.) | |
| 18. | Name, Designation and Address of the contact person to whom all references shall be made regarding this RFP: | |

Please submit the relevant proofs for all the details mentioned above along with your Bid response

Authorized Signatory
Name
Seal

## 6.3 Format of sending pre-bid queries

All queries for the pre-bid meeting needs to be submitted in the following format (both soft copy and hard copy) as mentioned in "Key Events and Dates" clause

*Ref*: RFP Notification number: **MMRC/IT/RFP DC-DR/71**

<table>
<tr><th colspan="5">Bidder's Request For Clarification</th></tr>
<tr><td colspan="3">Name and complete official address of Organization submitting query / request for clarification</td><td colspan="2">Telephone, Fax and E-mail of the organization<br>Tel:<br>Fax:<br>Email:</td></tr>
<tr><th>Sr. No.</th><th>Clause No.</th><th>Page No.</th><th>Content of RFP Requiring Clarification</th><th>Change Requested/ Clarification required</th></tr>
<tr><td>1</td><td></td><td></td><td></td><td></td></tr>
<tr><td>2</td><td></td><td></td><td></td><td></td></tr>
</table>

Signature:

Name of the Authorized signatory:

Company seal:

Date and Stamped

## 6.4 Format to Project Citation

| S No | Item | Details | Attachment Ref. Number |
|---|---|---|---|
| **1** | Name of the Project | | |
| **2** | Date of Work Order | | |
| **3** | Client Details | | |
| **4** | Scope of Work | | |
| **5** | Contract Value | | |
| **6** | Completion Date | | |

***Note: The Bidder is required to use above formats for all the projects referenced by the bidder for the Pre-Qualification and technical bid evaluation.***

## 6.5 Details of Manpower Resources Proposed

| S No | Proposed Position | Name of the Resource | Proposed Role | Highest Qualification | Total Experience (in years) | Total Relevant Experience for the proposed position (in years) |
|---|---|---|---|---|---|---|
| 1. | Project Manager | | | | | |
| 2. | Senior Solution Architect | | | | | |
| 3. | Disaster Recovery Specialist | | | | | |
| 4. | Server Administrator | | | | | |
| 5. | Network Support Engineer | | | | | |
| 6. | Database Administrator | | | | | |

### 6.5.1 Format for CV's of Proposed Manpower

A detailed profile of the key staff proposed for the MMRC project, is to be enclosed along with the Technical Proposal, in the format given below:

| Item | Description |
|---|---|
| Name | |
| Designation / Role | |
| Academic Qualifications | |
| Relevant Certification | |
| Total years of relevant experience | |
| Total number of similar project executed in the proposed role with brief details of each project | Name of assignment or Project |
| | Name of Client |
| | Years |
| | Location |
| | Main Project features |
| | Positions held |
| | Activities performed |

| Certifications | |
|---|---|
| I, the undersigned certify that: | |
| To the best of my knowledge and belief, this CV correctly describes me, my qualifications, and my experience. | |
| I understand that my willful misstatement described herein may lead to my disqualification or dismissal, if engaged. | |
| Name & Signature (Personnel) | Name & Signature (Authorized Representative) |
| | Date of signing |

## 6.6 Project Implementation Methodology

**The Bidder is required to submit the proposed technical solution in detail. Following should be captured in the explanation:**

a. The Overall approach to the Project
b. Details of Cloud Management Solution
c. A detailed description of the solution and solution approach
d. Implementation Methodology and Overall Solution Architecture and Details comprising of detailed license requirement
e. Strength of the Bidder to provide services including examples or case-studies of similar work
f. Project Organization and Management Plan
g. Extent of compliance with the specifications mentioned in the scope of work in the section 4 of the RFP
h. Project Monitoring and Communication Plan– Bidder's approach to project monitoring and communications among stakeholders
i. Change management methodology
j. The performance benchmark for the offered solution & services
k. The constraints, essentials and necessities if any for installation & commissioning of system
l. Implementation plan– Bidder's approach to implement the project
m. Risk Management Plan – Bidder's approach to identify, respond / manage and mitigate risks
n. Quality Control plan - Bidder's approach to ensure quality of work and deliverables
o. Escalation matrix during contract period
p. Disaster Recovery Plan

**Note:**

a. All the pages (documentary proofs and other documents that may be attached) should contain page numbers and would have to be uniquely serially numbered.

b. Inadequate information shall lead to disqualification of the bid.

## 6.7 Check-list for the documents for Pre-Qualification Envelope

### A. For Managed Service Provider (MSP)

| Sr. No. | Eligibility Criteria | Documents to be submitted | Submitted (Yes/No) | Details | |
|---|---|---|---|---|---|
| PQ1 | The MSP should be a company registered under the Companies Act, 2013 or the Companies Act, 1956 OR a Limited Liability Partnership (LLP) registered under the LLP Act, 2008 or Indian Partnership Act 1932 | Copy of Certificate of Incorporation/ Registration/ Partnership deed | | Document Name / Page Number | |
| | | Copy of PAN Card | | Document Name / Page Number | |
| | | Copy of GST Registration | | Document Name / Page Number | |
| PQ2 | The MSP should have minimum average annual turnover of Rs. 3.5 crore from Data Centre business in India for the last three financial years (FY 14-15, FY 15-16, FY 16-17) | Certificate from the Statutory Auditor clearly stating the Turnover from Data Centre services | | Document Name / Page Number | |
| PQ3 | The MSP should have successfully implemented /commissioned at least 1 (one) project of DC/DR with Cloud deployment with an order value of minimum Rs. 1.76 Cr hosted out of the proposed DC / DR facility in India | Work order + Completion Certificates from the client;<br>OR<br>Work Order + Self Certificate of Completion (Certified by the | | Project Name:<br>Client Name:<br>Project Value:<br>Project Date:<br>Document Submitted:<br>Work Order / Project Completion Certificate | Document Name / Page Number |

| Sr. No. | Eligibility Criteria | Documents to be submitted | Submitted (Yes/No) | Details | |
|---|---|---|---|---|---|
| | OR<br>at least 2 (two) projects of DC/DR with Cloud deployment with an order value of minimum Rs. 1.32 Cr hosted out of the proposed DC / DR facility in India<br>OR<br>at least 3 (three) projects of DC/DR with Cloud deployment with an order value of minimum Rs. 88 Lakhs hosted out of the proposed DC / DR facility in India<br>Note:<br>In case of an ongoing project, the percentage of work completed for must be at least 50%. | Statutory Auditor);<br>OR<br>Work Order + Phase Completion Certificate by client | | Project Name:<br>Client Name:<br>Project Value:<br>Project Date:<br>Document Submitted: Work Order / Project Completion Certificate | Document Name / Page Number |
| | | | | Project Name:<br>Client Name:<br>Project Value:<br>Project Date:<br>Document Submitted: Work Order / Project Completion Certificate | Document Name / Page Number |
| PQ4 | The MSP should not be debarred/ blacklisted by any Government/PSU in India as on date of submission of the Bid. | A self-certified letter signed by the Authorized Signatory of the Bidder as per Annexure A | | Document Name / Page Number | |

## B. For Cloud Service Provider (CSP)

| Sr. No. | Eligibility Criteria | Documents to be submitted | Submitted (Yes/No) | Details |
|---|---|---|---|---|

| | | | | |
|---|---|---|---|---|
| PQ1 | The CSP should be a company registered under the Companies Act, 2013 or the Companies Act, 1956 OR a Limited Liability Partnership (LLP) registered under the LLP Act, 2008 or Indian Partnership Act 1932. | Copy of Certificate of Incorporation/ Registration/ Partnership deed | | Document Name / Page Number |
| | | Copy of PAN Card | | Document Name / Page Number |
| | | Copy of GST Registration | | Document Name / Page Number |
| PQ2 | The Data Center facility must meet all of the following criteria: | | | |
| PQ 2(1) | Should confirm to Tier III standards/ and the certificate/rating should be valid at the time of bidding. | Valid Copy of the Tier III Certification, certified under TIA 942 or Uptime Institute certifications by a 3rd party | | Document Name / Page Number |
| PQ 2(2) | Data Center and Disaster Recovery Center Facilities must be certified for ISO 27001 / 27018 (year 2013 or above) and provide service assurance and effectiveness of Management compliant with ISO 20000 standards. | Valid Copy of the ISO 27001 / 27018, ISO 20000 Certification | | Document Name / Page Number |
| PQ3 | The OEM whose Cloud / Virtualization Solution are being proposed should have at least 10 implementations of the same product in third party Data Centers in India. The Bidder must be authorized by OEM | OEM certification for usage in at least 10 implementations in third party Data Centers in India. | | Document Name / Page Number |

| | | | | |
|---|---|---|---|---|
| | (Original Equipment Manufacturer) in India for Cloud Solution / Virtualization Solution offering | Manufacturer's authorization Form from OEM | | |
| PQ4 | The Cloud Service Provider shall be empaneled and audit compliant as per Ministry of Electronics and Information Technology (MeitY). | Letter of Empanelment / Certificate of Empanelment from MeitY (Empanelment should be current and applicable as on bid submission date) | | Document Name / Page Number |
| PQ5 | Proposed DR site should be in a different Seismic Zone than the current MMRC DC at Bandra Kurla Complex, Mumbai. | Letter from authorized signatory on the letter head of CSP mentioning the address of the proposed MeitY / Cert-in Certified Disaster Recovery Site. | | Document Name / Page Number |
| PQ6 | The Bidder should not be debarred/ blacklisted by any Government/PSU in India as on date of submission of the Bid. | A self-certified letter signed by the Authorized Signatory of the Bidder as per Annexure A | | Document Name / Page Number |

## 6.8 Check-list for the documents for Technical Evaluation

| # | Criteria | Documents Required | Self-Assessment Marks | Details | |
|---|---|---|---|---|---|
| TQ 1 | Experience of Bidder in offering cloud services(IaaS) in India or Globally<br>Maximum Marks 10<br>2-5 years : 6 marks<br>6-9 years : 8 marks<br>10+ years : 10 marks | Project Work order /Completion Certificates from the client stating Project Start date and Project End date | | Project Name:<br>Client Name:<br>Project Value:<br>Project Date:<br>Document Submitted: Work Order / Project Completion Certificate | Document Name / Page Number |
| TQ 2 | Tier Classification of the proposed Data Center, where cloud hosting is to be served from :<br>Maximum Marks 5<br>Tier III : 3 marks<br>Tier IV : 5 marks | Valid Copy of the Tier III or Tier V Certification, certified under TIA 942 or Uptime Institute certifications by a 3rd party | | Document Name / Page Number | |
| TQ 3 | Data Centre Uptime in Last 4 quarters<br>Maximum Marks 10<br><99.5% : 0 marks<br>99.5-99.9% : 5 marks<br>>99.9% : 10 marks | Self-undertaking along with system generated report | | Document Name / Page Number | |
| TQ 4 | Number of VMs running (active) in the DC of the bidder<br>Maximum Marks 10 | Self-undertaking along with report showing number of | | Document Name / Page Number | |

| | | | | | |
|---|---|---|---|---|---|
| | 200-400 VM's : 6 marks<br>401-600 VM's : 8 marks<br>>=601 VM's : 10 marks | VM's running from proposed DC/DR facility | | | |
| TQ 5 | Compliance to Functional Requirements<br>Maximum Marks 15<br>>95% - 15 marks<br>85-95% - 10 marks<br>70-85% - 5 marks | Compliance sheet as per section 4.11.2 to be submitted, signed and stamped by Authorized Signatory | | Document Name / Page Number | |
| TQ 6 | Project Manager Exp. in terms of Data Center Management, Cloud Solution Design and Management<br>Maximum Marks 10<br>8-11 years : 6 marks<br>12-15 years: 8 marks<br>>=16 years : 10 marks | CV for Proposed Resource | | Document Name / Page Number | |
| TQ 7 | MSP's experience in setting up IT Infra on cloud based DC/DR for minimum order value of Rs. 88 Lakhs hosted out of the proposed DC / DR facility in India<br>Maximum Marks 15<br>1 project : 3 marks<br>Every additional project: 3 marks, max. upto 15 marks | Project Work order and Completion Certificates | | Project Name:<br>Client Name:<br>Project Value:<br>Project Date:<br>Document Submitted: Work Order / Project Completion Certificate | Document Name / Page Number |
| TQ 8 | Technical Presentation<br>Maximum Marks 25 | | | Document Name / Page Number | |

| | | | | |
|---|---|---|---|---|
| | Bidders understanding of the project and Scope of Work – 5 marks | | | |
| | Technical Solution – 5 marks | | | |
| | Project Management Methodology and People / Resources – 5 marks | | | |
| | Demonstration of the cloud solution – 5 marks | | | |
| | Clarifications / Answers given to the Bid Evaluation Committee during the Presentation – 5 marks | | | |
| | Total Marks 100 | | | |

Note: MMRC shall evaluate all documents provided by bidders for technical evaluation and allocate marks which shall be final and binding upon the bidders.

# 7. Guidelines for Financial Proposal

## 7.1 Financial Proposal Cover Letter

(To be submitted on the Letterhead of the bidder)

Date: dd/mm/yyyy

To,

Executive Director (Electrical)
MMRC,
Bandra - Kurla Complex,
Bandra (East)
Mumbai—400 051

**Subject**: Submission of proposal in response to the RFP for Hiring of "Cloud based Disaster Recovery services" from Managed Service Provider at Mumbai Metro Rail Corporation (MMRC)

**Ref**: **MMRC/IT/RFP DC-DR/71**

Dear Sir,

We, the undersigned, offer to provide the services for "**Hiring of "Cloud based Disaster Recovery services" from Managed Service Provider at Mumbai Metro Rail Corporation (MMRC)"** *in* accordance with your Request for Proposal dated [*Insert Date*] and our Technical Proposal. Our attached Financial Proposal for is for the sum of [*Insert amount(s) in words and figures*]. We are aware that any conditional financial offer will be outright rejected by MMRC. 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 (180 days) from the date of submission of Bid.

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. We confirm that no Pre-Qualification deviations are attached here with this commercial offer. We remain,

Yours sincerely,
Authorized Signature [*In full and initials*]:
Name and Title of Signatory:
Date and Stamp of the signatory
Name of Firm:

## 7.2 Financial Proposal Instructions

1. MMRC may award entire scope or part of scope, mentioned in section 4.0, as MMRC deems fit.
2. MMRC does not guarantee Work order of any line item in part or whole or volume for the particular line items. The actual volume for the given items may be more or less. The payment shall be made based on unit cost quoted for the particular item on actual services and components is undertaken, and further no extra cost shall be made in any account till the contract period.
3. The bidder should fill rates for all the items mentioned here. If rate for any item is not mentioned then the bid will be rejected by MMRC.
4. All the prices are to be entered in Indian Rupees ONLY.
5. The Bidder needs to account for all Out of Pocket expenses due to Boarding, Traveling, Lodging and other related items.
6. The Rates should be exclusive of all taxes. Taxes shall be paid as actual at prevailing rates by MMRC at the time of releasing the payments.
7. The rates mentioned above shall be valid for the contract duration.

## 7.3 Financial Proposal Format

***Ref:*** **MMRC/IT/RFP DC-DR/71**

**Financial Proposal Format**

**Table A: Cost Breakdown of Services based on monthly (based on number of hours and days) charges**

| Sr. No. | Description | Unit | Quantity | Price | Taxes Applicable | Total Cost |
|---|---|---|---|---|---|---|
| **Virtual Machines - ERP** | | | | | | |
| 1. | Production Application DB 6 vCore, 64 GB RAM 1.4 TB disk size.* | Per Machine per Hour | 1 | | | |
| **Virtual Machines – e Office** | | | | | | |
| 2. | App Server 8 vCore 64 GB RAM 1 TB HDD RHEL 7.2 64 Bit* | Per Machine per Hour | 1 | | | |
| 3. | DB Server 6 vCore 64 GB RAM 500 GB HDD RHEL 7.2 64 Bit* | Per Machine per Hour | 1 | | | |
| 4. | Local DNS Server – Win Server 2008 2 vCore 16 GB RAM* | Per Machine per Hour | 1 | | | |
| **Storage** | | | | | | |
| 5. | Additional Storage | 100 GB SSD storage per Month (**As per data size**) | 1 | | | |

| Sr. No. | Description | Unit | Quantity | Price | Taxes Applicable | Total Cost |
|---|---|---|---|---|---|---|
| **Additional Components** | | | | | | |
| 6. | Additional vCPU | Nos | 1 | | | |
| 7. | Additional RAM 4 GB | Nos | 1 | | | |
| 8. | Additional RAM 8 GB | Nos | 1 | | | |
| 9. | Additional Storage 500 GB | Nos | 1 | | | |
| **Software and Licenses - ERP** | | | | | | |
| 10. | Operating System OEL 6.6 | Nos | 1 | | | |
| 11. | Oracle Virtual Machine | Nos | 1 | | | |
| 12. | Oracle Weblogic Suite | NUP<br>Named User Plus Perpetual | 30 | | | |
| 13. | Oracle Database Enterprise Edition | NUP<br>Named User Plus Perpetual | 50 | | | |
| **Software and Licenses – E Office** | | | | | | |
| 14. | Operating System RHEL 7.2 | Nos | 1 | | | |

| Sr. No. | Description | Unit | Quantity | Price | Taxes Applicable | Total Cost |
|---|---|---|---|---|---|---|
| 15. | OS - Windows Server 2008 R2 Enterprise Edition 64 Bit | Nos | 1 | | | |
| 16. | RDBMS – PGSQL | Nos | 1 | | | |
| **Security & Firewall** | | | | | | |
| 17. | Web Application Firewall | Nos | 1 | | | |
| 18. | Public IPs<br>(5 IP's to be included at no cost) | Nos | 1 | | | |
| **Total Cost** | | | | **A1** | | |

**Total Cost A1 shall be entered in Summary Table below**

**Note:**

- In case of a particular Instance Type is not available, near or equivalent instance cost to be provided.
- The OS version shall be n, n-1 or a specific version and type as per MMRC's Application requirement.
- Bidder has to ensure Cloud Services (VMs provided) should be on Pay per use on hourly, monthly basis and the MMRC would pay only for the actual usage.

**Table B: Cost towards Support on a yearly basis**

| Sr. No | Particulars | Per Year Cost | Taxes Applicable | Total Amount |
|---|---|---|---|---|
| 1. | Yearly Support Cost | B1 | | |

**Total Cost B1 shall be entered in Summary Table below**

**Table C: Cost Breakdown for 10 Mbps Connectivity from DC at MMRC to DR for 5 years on monthly basis**

| Sr. No | Particulars | Per Month Cost | Taxes Applicable | Total Amount |
|---|---|---|---|---|
| 1. | 10 Mbps Connectivity | C1 | | |

**Total Cost C1 shall be entered in Summary Table below**

**Table D: Consolidated Cost Summary**

| # | Description | Total Cost excluding taxes for 5 years (in Rs.)<br>(Monthly Cost x 60 / Yearly Cost x 5) | Total Applicable Taxes (in Rs.) | Total Amount<br>(in Rs.) |
|---|---|---|---|---|
| 1. | Cloud Services – Cost for pre-production and production environment for 5 years (on demand pricing)(from above table A) | A2=A1 x 60 | A3 | A = A2 + A3 |
| 2. | Cost towards Support from CSP for 5 years (from above table B) | B2=B1 x 5 | B3 | B = B2 + B3 |
| 3. | Cost towards 10 Mbps Connectivity from MMRC DC to DR for 5 years (from above table C) | C2=C1 x 60 | C3 | C = C2 + C3 |
| | Grand Total | | | GT=A+B+C |

Note: Grand Total shall be used for Financial Evaluation

# 8. ANNEXURES

## Annexure A: Format for Declaration by the bidder for not being Blacklisted /Debarred

(To be submitted on the Letterhead of the responding company)

Date: dd/mm/yyyy

To
Executive Director (Electrical)
MMRC,
Bandra - Kurla Complex
Bandra (East)
Mumbai—400 051

**Subject:** Declaration for not being debarred / black-listed by Central / any Government or PSU in India as on the date of submission of the bid

**Tender Reference No: MMRC/IT/RFP DC-DR/71**

Dear Sir,

I, authorized representative of ______________________, hereby solemnly confirm that the Company ______________________ is not debarred /blacklisted by any Government or PSU for any reason as on last date of submission of the Bid. In the event of any deviation from the factual information/ declaration, MMRC, Government of Maharashtra reserves the right to reject the Bid or terminate the Contract without any compensation to the Company and forfeiture of Earnest Money Deposit and/or Security Deposit

Thanking you,

Yours faithfully,

______________________________

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

# Annexure B: Performance Security - Bank Guarantee Format

For Contract Performance Bank Guarantee

***Ref:* MMRC/IT/RFP DC-DR/71**

Date: _______________

Bank Guarantee No.: __________________

To

Executive Director (Electrical)
MMRC,
Bandra - Kurla Complex
Bandra (East)
Mumbai—400 051

Dear Sir,

PERFORMANCE BANK GUARANTEE – For MMRC <Project Name>

WHEREAS
M/s. (name of Bidder), a company registered under the Companies Act, 1956, having its registered and corporate office at (address of the Bidder), (hereinafter referred to as "our constituent", which expression, unless excluded or repugnant to the context or meaning thereof, includes its successors and assigns), agreed to enter into a Contract dated …….. (Hereinafter, referred to as "Contract") with you for "**Hiring of "Cloud based Disaster Recovery services" from Managed Service Provider at Mumbai Metro Rail Corporation (MMRC)**", in the said Contract.

We are aware of the fact that as per the terms of the Contract, M/s. (name of Bidder) is required to furnish an unconditional and irrevocable Bank Guarantee in your favor for an amount of 10% of the Total Contract Value, and guarantee the due performance by our constituent as per the Contract and do hereby agree and undertake to pay any and all amount due and payable under this bank guarantee, as security against breach/ default of the said Contract by our Constituent.

In consideration of the fact that our constituent is our valued customer and the fact that he has entered into the said Contract with you, we, (name and address of the bank), have agreed to issue this Performance Bank Guarantee.

Therefore, we (name and address of the bank) hereby unconditionally and irrevocably guarantee you as under:

In the event of our constituent committing any breach / default of the said Contract, and which has not been rectified by him, we hereby agree to pay you forthwith on demand such sum/s not exceeding the sum of 10% of the Total Contract Value i.e.,…………..<in words> without any demur.

Notwithstanding anything to the contrary, as contained in the said Contract, we agree that your decision as to whether our constituent has made any such default(s) / breach(es), as aforesaid and the amount or amounts to which you are entitled by reasons thereof, subject to the terms and conditions of the said Contract, will be binding on us and we shall not be entitled to ask you to establish your claim or claims under this Performance Bank Guarantee, but will pay the same forthwith on your demand without any protest or demur.

This Performance Bank Guarantee shall continue and hold good till 6 months after completion of the Contract Period, subject to the terms and conditions in the said Contract.

We bind ourselves to pay the above said amount at any point of time commencing from the date of the said Contract until 6 months after the completion of Contract Period.

We further agree that the termination of the said Agreement, for reasons solely attributable to our constituent, virtually empowers you to demand for the payment of the above said amount under this guarantee and we would honor the same without demur.

We hereby expressly waive all our rights: Requiring to pursue legal remedies against MMRC; and For notice of acceptance hereof any action taken or omitted in reliance hereon, of any defaults under the Contract and any resentment, demand, protest or any notice of any kind.

We the Guarantor, as primary obligor and not merely Surety or Guarantor of collection, do hereby irrevocably and unconditionally give our guarantee and undertake to pay any amount you may claim (by one or more claims) up to but not exceeding the amount mentioned aforesaid during the period from and including the date of issue of this guarantee through the period.

We specifically confirm that no proof of any amount due to you under the Contract is required to be provided to us in connection with any demand by you for payment under this guarantee other than your written demand.

Any notice by way of demand or otherwise hereunder may be sent by special courier, telex, fax, registered post or other electronic media to our address, as aforesaid and if sent by post, it shall be deemed to have been given to us after the expiry of 48 hours when the same has been posted. If it is necessary to extend this guarantee on account of any reason whatsoever, we undertake to extend the period of this guarantee on the request of our constituent under intimation to you.

This Performance Bank Guarantee shall not be affected by any change in the constitution of our constituent nor shall it be affected by any change in our constitution or by any amalgamation or absorption thereof or therewith or reconstruction or winding up, but will ensure to the benefit of you and be available to and be enforceable by you during the period from and including the date of issue of this guarantee through the period.

Notwithstanding anything contained hereinabove, our liability under this Performance Guarantee is restricted to 10% of the Contract Value, and shall continue to exist, subject to the terms and conditions contained herein, unless a written claim is lodged on us on or before the aforesaid date of expiry of this guarantee.

We hereby confirm that we have the power/s to issue this Guarantee in your favor under the Memorandum and Articles of Association / Constitution of our bank and the undersigned is / are the recipient of authority by express delegation of power/s and has / have full power/s to execute this guarantee under the Power of Attorney issued by the bank in your favor.

We further agree that the exercise of any of your rights against our constituent to enforce or forbear to enforce or any other indulgence or facility, extended to our constituent to carry out the contractual obligations as per the said Contract, would not release our liability under this guarantee and that your right against us shall remain in full force and effect, notwithstanding any arrangement that may be entered into between you and our constituent, during the entire currency of this guarantee.

Notwithstanding anything contained herein:

Our liability under this Performance Bank Guarantee shall not exceed 10% of the Total Contract Value. This Performance Bank Guarantee shall be valid only from the date of signing of Contract to 180 days after the End of Contract Period; and

We are liable to pay the guaranteed amount or part thereof under this Performance Bank Guarantee only and only if we receive a written claim or demand on or before 180 days after the completion of Contract Period.

Any payment made hereunder shall be free and clear of and without deduction for or on account of taxes, levies, imports, charges, duties, fees, deductions or withholding of any nature imposts.

This Performance Bank Guarantee must be returned to the bank upon its expiry. If the bank does not receive the Performance Bank Guarantee within the above-mentioned period, subject to the terms and conditions contained herein, it shall be deemed to be automatically cancelled.

This guarantee shall be governed by and construed in accordance with the Indian Laws and we hereby submit to the exclusive jurisdiction of courts of Justice in India for the purpose of any suit or action or other proceedings arising out of this guarantee or the subject matter hereof brought by you may not be enforced in or by such count.

Dated …………………… this ………. Day ………… 2017.
Yours faithfully,

For and on behalf of the …………… Bank,

(Signature)
Designation
(Address of the Bank)
Note:

This guarantee will attract stamp duty as a security bond.

A duly certified copy of the requisite authority conferred on the official/s to execute the guarantee on behalf of the bank should be annexed to this guarantee for verification and retention thereof as documentary evidence in the matter.

# Annexure C: Non-Disclosure Agreement

[Company Letterhead]

This AGREEMENT (hereinafter called the "Agreement") is made on the [day] day of the month of [month], [year], between, Mumbai Metro Rail Corporation on the one, (hereinafter called the "MMRC") and, on the other hand, [Name of the Bidder] (hereinafter called the "Bidder") having its registered office at [Address]

WHEREAS

1. The "MMRC" has issued a public notice inviting various organizations for provision of Hiring of "Cloud based Disaster Recovery Services" from Managed Service Provider at Mumbai Metro Rail Corporation (MMRC) , Mumbai (hereinafter called the "Project") of the MMRC;

2. The Bidder, having represented to the "MMRC" that it is interested to bid for the proposed Project,

3. The MMRC and the Bidder agree as follows:

a) In connection with the "Project", the MMRC agrees to provide to the Bidder a detailed document on the Project vide the Request for Proposal document. The Request for Proposal contains details and information of the MMRC operations that are considered confidential.

b) The Bidder to whom this information (Request for Proposal) is disclosed shall –

i. hold such information in confidence with the same degree of care with which the Bidder protects its own confidential and proprietary information;

ii. restrict disclosure of the information solely to its employees, other member with a need to know such information and advice those persons of their obligations hereunder with respect to such information;

iii. use the information only as needed for the purpose of bidding for the Project;

iv. except for the purpose of bidding for the Project, not copy or otherwise duplicate such information or knowingly allow anyone else to copy or otherwise duplicate such information; and

v. undertake to document the number of copies it makes

vi. on completion of the bidding process and in case unsuccessful, promptly return to the MMRC, all information in a tangible form or destroy such information

4. The Bidder shall have no obligation to preserve the confidential or proprietary nature of any information which:

a) was previously known to the Bidder free of any obligation to keep it confidential at the time of its disclosure as evidenced by the Bidder’s written records prepared prior to such disclosure; or
b) is or becomes publicly known through no wrongful act of the Bidder; or
c) is independently developed by an employee, agent or contractor of the Bidder not associated with the Project and who did not have any direct or indirect access to the information.

5. The Agreement shall apply to all information relating to the Project disclosed by the MMRC to the Bidder.

6. MMRC will have the right to obtain an immediate injunction enjoining any breach of this Agreement, as well as the right to pursue any and all other rights and remedies available at law or in equity for such a breach.

7. MMRC reserves the right to share the information received from the bidder under the ambit of RTI Act.

8. Nothing contained in this Agreement shall be construed as granting or conferring rights of license or otherwise, to the Bidder, on any of the information. Notwithstanding the disclosure of any information by the MMRC to the Bidder, the MMRC shall retain title and all intellectual property and proprietary rights in the information. No license under any trademark, patent or copyright, or application for same that are now or thereafter may be obtained by the MMRC is either granted or implied by the conveying of information. The Bidder shall not alter or obliterate any trademark, trademark notice, copyright notice, confidentiality notice or any notice of any other proprietary right of the MMRC on any copy of the information, and shall reproduce any such mark or notice on all copies of such information.

9. This Agreement shall be effective from the date of signing of this agreement and shall continue perpetually.

10. Upon written demand of the MMRC, the Bidder shall (i) cease using the information, (ii) return the information and all copies, notes or extracts thereof to the MMRC forthwith after receipt of notice, and (iii) upon request of the MMRC, certify in writing that the Bidder has complied with the obligations set forth in this paragraph.

11. This Agreement constitutes the entire Agreement between the MMRC and the Bidder relating to the matters discussed herein and supersedes any and all prior oral discussions and/or written correspondence or agreements between the two parties. This Agreement may be amended or modified only with the mutual written consent of the parties. Neither this Agreement nor any right granted hereunder shall be assignable or otherwise transferable.

12. Confidential information is provided "As-Is". In no event shall the MMRC be liable for the accuracy or completeness of the confidential information.

13. This agreement shall benefit and be binding upon the MMRC and the Bidder and their respective subsidiaries, affiliate, successors and assigns.

14. This agreement shall be governed by and construed in accordance with the Indian laws.

For and on behalf of the Bidder

(Signature)
(Name of the authorized Signatory)
Designation :
Date :
Time :
Seal :
Business Address

# Annexure D: Declaration of Data Security

To,
Executive Director (Electrical)
MMRC,
Bandra - Kurla Complex
Bandra (East)
Mumbai—400 051

Dear Sir,

We....................................................... who are established and reputable bidder having office at............................... do hereby certify that MMRC shall have absolute right on the digital data and output products processed / produced by us. We shall be responsible for security / safe custody of data during processing.

We also certify that the data will not be taken out of the MMRC's premises on any media. The original input data supplied to us by MMRC and output products processed / produced from input data will not be passed on to any other Service Provider (SP) or individual other than the authorized person of MMRC. We shall abide by all security and general instructions issued by MMRC from time to time.

We also agree that any data from our computer system will be deleted in the presence of MMRC official after completion of the project task.

Thanking you,

Yours faithfully,

# Annexure E: Power of Attorney

Know by all men by these presents, We______________________ (Name of the Bidder and address of their registered office) do hereby constitute, appoint and authorize Mr. / Ms______________________ (name and residential address of Power of attorney holder) who is presently employed with us and holding the position of ______________________ as our Attorney, to do in our name and on our behalf, all such acts, deeds and things necessary in connection with or incidental to our Proposal for the **"Request for Selection for Hiring of "Cloud based Disaster Recovery services" from Managed Service Provider at Mumbai Metro Rail Corporation (MMRC)"**, including signing and submission of all documents and providing information / responses to the MMRC, representing us in all matters before MMRC, and generally dealing with the MMRC in all matters in connection with our Proposal for the said Project.

We hereby agree to ratify all acts, deeds and things lawfully done by our said Attorney pursuant to this Power of Attorney and that all acts, deeds and things done by our aforesaid Attorney shall and shall always be deemed to have been done by us.

For ________________________
Name:
Designation:
Date:
Time:
Seal:
Business Address:

Accepted,
______________________ (Signature)
(Name, Title and Address of the Attorney)

Note:

- The mode of execution of the Power of Attorney should be in accordance with the procedure, if any, laid down by the applicable law and the charter documents of the executant(s) and when it is so required the same should be under common seal affixed in accordance with the required procedure.
- The Power of Attorney shall be provided on Rs.100/- stamp paper.
- The Power of Attorney should be supported by a duly authorized resolution of the Board of Directors of the Bidder authorizing the person who is issuing this power of attorney on behalf of the Bidder.

## Annexure F: Agreement Format

THIS AGREEMENT made the ….. day of …… 2017 BETWEEN Mumbai Metro Rail Corporation Limited having its office at Executive Director (Electrical, 5th Floor, MMRDA Old Building, Bandra Kurla Complex, Bandra (East), Mumbai—400 051 (hereinafter referred to as “MMRC”) which expression shall unless repugnant to the context or meaning thereof mean and be deemed to include its authorized agents, representatives and permitted assigns of the First Part.

AND

M/s <Name of the Bidder>having its office at <office address of the bidder> which expression shall unless repugnant to the context or meaning thereof mean and be deemed to include their successors and permitted assigns of the Second Part.

WHEREAS the contractor has tendered for providing services to MMRC as per the terms and conditions mentioned in the Request for Proposal (from herein after referred to as “RFP”) “For Hiring of “Cloud based Disaster Recovery Services” from Managed Service Provider at Mumbai Metro Rail Corporation (MMRC)” dated <date of release of RFP> and the all subsequent corrigendum’s published document, as per the Commercial Bid submitted in response to the RFP dated <date of release of RFP >. Whereas such tender has been accepted and the contractor has provided Bank Guarantee to MMRC, Mumbai for the sum of Rs. <amount of the bid>.

NOW IT IS HEREBY AGREED between the parties hereto as follows:
The contractor has accepted the contract on the terms and conditions set out in the RFP No: <Ref no of RFP> issued on <date of issue of RFP> and all subsequent communications through letters / emails and clarifications/corrigendum issued which shall hold good during period of this agreement.

Refund of deposit shall be based on the timelines, terms and conditions as has been specified in the RFP/LoI and shall form a part of the contract. In absence of any timeline specified the deposit shall after the expiration of 180 days from the date of completion of the contract, be returned to the contractor but without interest and after deducting there from any sum due by the contractor to MMRC under the terms and conditions of this agreement.

This agreement shall remain in force until the expiry of <duration of the contract> from the date of entering into the contract, but MMRC may cancel the contract at any time upon giving 30 days’ notice in writing without compensating the Service Provider.

All terms and conditions as specified in the RFP, clarifications / corrigendum issued in regards to the RFP <ref no RFP> as has been mentioned above in the document shall stand enforce unless has been expressly agreed to in writing by both the parties.

The Contractor shall be responsible to abide and shall be liable to deliver the requirements/deliverables as has been specified to in the RFP, clarifications / corrigendum issued in regards to the RFP. No. <ref no RFP> and Letter of Acceptance No: <LoI number> dated <date>.

IN WITNESS whereof the said Contractor hath set his hand hereto and MMRC has affixed his hand and seal thereto the day and year first above written.

| | |
|---|---|
| Signed, sealed and delivered | Signed, sealed and delivered |
| By | By |
| Executive Director (Electrical) | For and on behalf of |
| For and on behalf of | M/s <Name of Bidder> |
| Mumbai Metro Rail Corporation Limited | |
| Witnesses: | Witnesses: |
| (1) | (1) |
| (2) | (2) |

***********************End of Document*************************