



Municipal Corporation of Greater Mumbai

## **REQUEST FOR PROPOSAL**

for

" Selection of Service Provider for Implementation  
of IT Audit at MCGM”

**Tender ID : 7200011279**

Prepared By:

Checked By:

Verified By:

Approved By:

--sd--

--sd--

--sd--

--sd--

M/s PwC

SSA/JSA

Manager (IT)

Director (IT)

**1 Contents**

1	Invitation of Bid .....	6
1.1	Project Background.....	6
1.2	Objectives .....	6
1.3	Bid Document Notice.....	7
1.4	Bid Invitation .....	8
2	Pre-Qualification Criteria .....	9
3	Instructions to Bidder.....	11
3.1	Bid Data Sheet.....	11
3.2	Purpose of the Bid Document .....	12
3.3	Cost of Bid Document.....	13
3.4	Bidder Registration and Instructions .....	13
3.5	Bid Preparation Cost.....	13
3.6	Pre-bid Meeting .....	14
3.7	Amendment of Bid Document .....	15
3.8	Rights to Terminate the Process .....	15
3.9	Earnest Money Deposit (EMD) and Refund .....	15
3.10	Solvency Certificate.....	17
3.11	Submission of Bids.....	17
3.12	Process for Submission.....	18
3.13	Site Visit.....	19
3.14	Language of the Bid .....	19
3.15	Bid Submission Format .....	19
3.16	Documents Comprising the Bid .....	19
3.17	Evaluation Process.....	21
3.18	Opening of Bid .....	22
3.19	Evaluation of Technical Bid .....	22
3.20	Opening of Commercial Bid .....	28
3.21	Selection Method .....	29
3.22	Right to Accept or Reject Any or All Bids .....	29
3.23	Notification of Award and Signing of Contract .....	30
3.24	Performance Bank Guarantee .....	31
3.25	Failure to agree with the Terms and Conditions of the Bid/Contract .....	32
3.26	Terms and Conditions of the Bid .....	32
3.27	Legal and Stationery Charges.....	32
3.28	Stamp Duty.....	33

---

4	Scope of Work .....	35
4.1	Introduction .....	35
4.2	Preliminary Review.....	35
4.2.1	IT Infrastructure Audit.....	35
4.2.2	Email Security Audit.....	43
4.2.3	Digital Forensics Readiness Assessment.....	43
4.2.4	Cloud Security Review .....	44
4.2.5	Process Review.....	45
4.2.6	SAP & Non-SAP Application Audit.....	55
4.2.7	IT Audit for locations.....	63
4.3	Compliance Review.....	65
4.3.1	Post Implementation (Compliance) Review: .....	65
4.4	Other Components and Reporting.....	65
4.4.1	Description of applications and details on in-scope IT infrastructure components .....	67
4.4.2	Details of the existing IT landscape and Infrastructure of MCGM:.....	71
4.4.3	Standards to be followed during review/ audit.....	77
4.4.4	Deliverables.....	78
4.4.5	Minimum Qualifications & Experience for key Resources.....	80
4.4.6	Operational Procedure .....	81
5	Service Level Agreements .....	84
5.1	Maximum Penalty .....	84
5.2	Risk Purchase Clause .....	84
6	Payment Terms and Schedule .....	86
7	Annexure I: Pre-Qualification Documents .....	87
7.1	Pre-Qualification Cover Letter .....	87
7.2	Format to Share Bidder's Particulars .....	89
7.3	Format to Share Project Status .....	91
7.4	Format for Declaration by the Bidder for not being Blacklisted / Debarred .....	92
7.5	Performance Bank Guarantee .....	94
8	Annexure II: Instructions and Technical Bid Document Formats.....	97
8.1	General Instructions .....	97
8.2	Format to Share Project Details.....	98
8.3	Details of Manpower Resources Proposed .....	99
8.4	CV of the Proposed Key Manpower .....	99
9	Annexure III: Commercial Bid Formats .....	102
9.1	Commercial Bid Cover Letter .....	102
9.2	Commercial Bid Format and Instructions.....	105

---

9.3	Commercial Proposal Format & Instruction .....	112
9.4	Commercial Format (Online).....	114
10	Annexure IV: List of Approved Banks .....	115
11	Annexure V: Authorization Letter for Attending Bid Opening .....	118
12	Annexure VI: Draft Contract Agreement.....	119
12.1	Definitions, Interpretations and Other Terms.....	120
12.2	Interpretations .....	124
12.3	Term of the Contract Agreement .....	126
12.4	MCGM's Decision .....	127
12.5	Delegation .....	127
12.6	Communication.....	127
12.7	Other Bidders .....	127
12.8	Personnel.....	128
12.9	MCGM's and Selected Agency's Risks .....	128
12.10	MCGM's Risks.....	128
12.11	Selected Agency's Risks .....	128
12.12	Management Meetings .....	129
12.13	Tests.....	129
12.14	Variations .....	129
12.15	Payment for Variations.....	130
12.16	Operation and Maintenance Manuals .....	130
12.17	Compliance with Labour Regulations.....	130
12.18	Clarification.....	131
12.19	Format & Signing of Application .....	131
12.20	Marking of Application.....	132
12.21	Clarification of Financial Bids.....	132
12.22	Official Secrecy.....	132
12.23	Subsequent Legislation .....	132
12.24	Patent, Rights & Royalties.....	133
12.25	Payment, Taxes & Claims .....	133
12.26	Receipts to be signed in firm's name by any one of the partners.....	133
12.27	Proprietary data .....	134
12.28	Correspondence with the Selected Agency.....	134
12.29	Taxes.....	134
12.30	Contract Execution .....	135
12.31	Bribery and Insolvency.....	135
12.32	Fees.....	136

12.33	Use and Acquisition of Assets during the term .....	136
12.34	Security and safety .....	137
12.35	Indemnity .....	138
12.36	Third Party Claims.....	139
12.37	Publicity.....	141
12.38	Warranties.....	141
12.39	Force Majeure .....	143
12.40	Resolution of Disputes .....	143
12.41	Risk Purchase Clause .....	144
12.42	Conflict of Interest .....	145
12.43	Data Ownership .....	145
12.44	Fraud and Corruption.....	145
12.45	Exit Management.....	146
12.46	Termination of contract.....	148
12.47	Termination for Convenience .....	149
12.48	Miscellaneous.....	149
12.49	Applicable Law .....	155
12.50	Stamp Duty Payment .....	156
13	Annexure VII: Draft Non-Disclosure Agreement.....	158
14	Annexure VIII: Irrevocable Undertaking .....	164

➤ **Glossary**

<b>Abbreviations &amp; Acronyms</b>	<b>Description</b>
BEC	Bidder's Evaluation Committee
MCGM	Municipal Corporation of Greater Mumbai
EMD	Earnest Money Deposit
GoI	Government of India
BG	Bank Guarantee
CA	Contract Agreement
HoD	Head of Department
PAN	Permanent Account Number
PDF	Portable Document Format
RFP	Request for Proposal
VAT	Value Added Tax
IT	Information Technology
LOI	Letter of Intent
MCGM	Municipal Corporation of Greater Mumbai
SA	Selected Agency
SLA	Service Level Agreement
Bid/RFP/Tender	This refers to the bid process conducted by MCGM and the bid submitted by the successful Bidder, along with the subsequent clarifications and undertakings, if any for the ' <b>Selection of Service Provider for Implementation of IT Audit at MCGM</b> '; the words have been used interchangeably.

## **1 Invitation of Bid**

### **1.1 Project Background**

The Municipal Corporation of Greater Mumbai (MCGM) caters to the needs of its citizens with the help of a complex multi-departmental set-up and network of twenty-four decentralised Ward Administrations. MCGM is set to embark on an ambitious computerisation initiative in order to increase operational efficiency and effectiveness, improve financial health, enhance responsiveness to citizen's needs and result in transparency.

As part of this initiative, MCGM has already digitized processes like Octroi collection, Property Tax collection, Water Bill Collection, AutoDCR, GIS, e-office and other systems. However, in order to validate the correctness of system calculations, assessing the operational integrity of an automated process, verifying that confidential data is not exposed to unauthorized individuals, assessing the security configuration of applications, operating systems, databases and network devices, checking correctness, accuracy and confidentiality of integration with SAP systems and migration with cloud infrastructure and/or multiple combinations of these and other systems-related matters of importance, MCGM decided to conduct **IT Audit** which comprises of Systems Audit and Security Audit of IT Infrastructure at MCGM and other associated reviews.

MCGM intends to avail the services of a CERT-In empanelled agency to conduct an IT System Audit of MCGM's IT Infrastructure & Applications. The selected bidder shall be responsible for the following activities:

- The vendor shall perform an in-depth audit of the environment, identifying threat & attack vectors and analyzing gaps/ impacts/ risks to MCGM
- The vendor shall provide an approach or framework for collecting and assessing the information necessary for identifying gaps/ risks which are not covered by currently deployed controls.
- Within this approach or framework, the vendor shall:
  - Define a project plan for the full length of the engagement, including high level milestones (including the assessment, recommendations and treatments)
  - Define validation of the extensive documentation
  - Define whether and how many facilitated sessions will be required
  - Draft agendas for each session

Define the key people required and the deliverables

### **1.2 Objectives**

The objective of this project is to conduct IT systems audit for the following landscape:

1. IT Infrastructure Audit
2. SAP Applications Audit
3. Non-SAP Applications Audit
4. Location based audit

The Security Audit of IT infrastructure would ensure the following:

- Adherence to IT processes
- Ensure preventive measures for physical and environmental security
- Verify and ensure the secure configuration of IT infrastructure components
- Analysis of existing capacity, performance, redundancy and layout of network

### **1.3 Bid Document Notice**

1. This bid Document is being published by the Director of Information Technology Department, MCGM, for **“Selection of Service Provider for Implementation of IT Audit at MCGM”**.
2. Bidder agencies are advised to study this bid document carefully before submitting their bids in response to the Bid Notice. Submission of a bid in response to this notice shall be deemed to have been done after careful study and examination of this document with full understanding of its terms, conditions and implications.
3. This bid document is not transferable.
4. The complete bidding document has been published on <https://portal.mcgm.gov.in> for the purpose of downloading. The downloaded bidding document shall be considered valid for participation in the electronic bidding process (eProcurement) subject to the submission of required tender/ bidding document fee and EMD.
5. Bidders who wish to participate in this bidding process must register on <https://portal.mcgm.gov.in>
6. To participate in online bidding process, Bidders must procure a Digital Signature Certificate (Class - III) as per Information Technology Act-2000 using which they can digitally sign and encrypt their electronic bids. Bidders can procure the same from any CCA approved certifying agency. Bidders who already have a valid Digital Signature Certificate (DSC) need not procure a new DSC.
7. This is a two-packet tendering procedure.
8. Bidder (authorized signatory) will submit their offer online in electronic formats of technical (including prequalification documents) and financial proposal.
9. MCGM will not be responsible for delay in online submission due to any reason. For this, bidders are requested to upload the complete bid proposal, well in advance so as to avoid issues like slow speed or any other unforeseen problems. For queries related to eTender, kindly contact; Tel: 022-24811275, Email: [etendering.it@mcgm.gov.in](mailto:etendering.it@mcgm.gov.in)



#### **1.4 Bid Invitation**

Office of the Director, Information Technology Department, MCGM, invites bidders to submit their technical bids and financial offers for the “**Selection of Service Provider for Implementation of IT Audit at MCGM**”.

## 2 Pre-Qualification Criteria

#	Pre-Qualification Criteria	Proof Document Required
1.	The bidder should be a company registered under Indian Companies Act, 1956 or a partnership firm registered under Indian Partnership Act, 1932 or a Proprietorship firm or LLP.	Certified copy of Partnership Deed/Certified copy of Certificate of Incorporation/ Registration Certificate
2.	The bidder must have a valid CERT-In empanelment as on date of bid opening.	Certificate of CERT-In empanelment
3.	Also, the bidder should have a minimum average annual turnover of Rs. 6 Crores in India over the last three consecutive financial years (2017-18, 2018-19, 2019-2020), from Security Audit & Security Consulting Services.  The bidder should have a positive net worth as on 31/03/2021	Copy of the audited Balance Sheet and Profit & Loss Statement of the company and Certificate from the Chartered Accountant clearly stating the turnover of Rs. 6 Crores in India over the last three financial years (2018-19, 2019-20, 2020-21) from Security Audit & Security Consulting Services.
4.	The Bidder must have executed at least three assignments in each area in last 5 years from the date of publication of bid: <ul style="list-style-type: none"> <li>• Systems Audit for SAP and other ERP applications</li> <li>• Security audit for IT Infrastructure</li> <li>• IT Process Review</li> </ul>	Copy of Work Order and Client certificate signed by a competent authority clearly stating the scope, applicable areas of audit, current status and the contact details of the reference person.
5.	Registered for Service Tax/GST and Income Tax in India	Service Tax/GST Registration and latest Income Tax Certificate (ITR) along with PAN Card Copy
6.	The bidder should not have been blacklisted by Central Government or any State Government organization / department/any Municipal Corporation in India at the time of submission of the Bid	Declaration letter by bidder as per format given in the Bid Document
7.	The Bidder should have or shall be ready to set up a project office in Mumbai Metropolitan Region (MMR).	Rental Agreement/ Utility Bill in the name of the company/Sale Deed or Declaration that the office will be set-up within a period of 30 days

#	Pre-Qualification Criteria	Proof Document Required
		from the date of issuance of Letter of Intent.
8.	<p>The Bidder must have at least 30 employees (posted in India) with more than 3 years of experience in Information Security and employed for more than 6 months in the present company as on date of submission of its response and their certifications need to be valid on that date, out of which:</p> <ul style="list-style-type: none"> <li>a) 10 should have passed examination for qualifications such as ISO 27001 Lead Auditors and/or ISO 27001 Lead Implementers from an accredited certifying agency.</li> <li>b) 10 should be CISA/CISSP qualified</li> <li>c) 10 should be OSCP/ CEH/ GCIH / CCNA / CCNP Certified</li> </ul>	<p>List of resources certified by the HR mentioning the name, qualifications, total experience, certification, certification validity date and date of joining of the resources.</p>

Please note that

- The agency should be competent in undertaking all the categories of audit as mentioned in Scope of Work
- Consortium and Sub contracting are not allowed

### 3 Instructions to Bidder

#### 3.1 Bid Data Sheet

#	Information	Details
<b>A. Introduction</b>		
1.	Project Name	Implementation of IT Audit at MCGM
2.	Bid Document reference No and start date	7200011279 dtd. 30.09.2021
3.	Tender Type	Open Tender via e-Tendering system
4.	Tender Fee + GST	INR 9400/- + 2.5% CGST + 2.5% SGST
5.	Tender Download Due Date	<b>Date: 28.10.2021</b>
6.	Earnest Money Deposit (EMD)	INR 2,27,700/-
7.	EMD Submission Due Date & Time	<b>28.10.2021 04:00 pm</b>
8.	Bank Solvency Certificate	INR 8 lakhs
9.	Mode of Payment of EMD	Online
<b>B. Preparation of Bids</b>		
10.	Language of Bid	English
11.	Bid Validity Period	180 Days from the Date of Opening the Bid
12.	Bank Guarantee (as security deposit)	10% of contract value
13.	Security Deposit Validity Period	6 months after expiry of contract period
<b>C. Pre-bid Meeting</b>		
14.	Last date for submission of queries for clarifications	<b>06.10.2021 04:00 pm</b>
15.	Query Submission	Online in the prescribed format only
16.	Date, Time and Venue for Pre-Bid meeting	<b>07.10.2021 03:00 pm</b> Municipal Corporation of Greater Mumbai, IT Department, Worli Data Centre, Gr. Floor, Eng. Hub Bldg., Dr. E. Moses Road, Worli, Mumbai – 400018

#	Information	Details
17.	Contact Person for clarification of Queries	<b>Manager-01 (IT)</b> Municipal Corporation of Greater Mumbai, IT Department, Worli Data Centre, Gr. Floor, Eng. Hub Bldg., Dr. E. Moses Road, Worli, Mumbai – 400018
18.	Contact Information	<b>E-mail:</b> <a href="mailto:manager01.it@mcgm.gov.in">manager01.it@mcgm.gov.in</a> <b>Phone No:</b> 9769993215
<b>D. Submission and Opening of Bids</b>		
19.	Last date (deadline) for receipt of proposals in response to Bid Document notice	<b>28.10.2021 04:00 pm</b> Online Bid Proposals Submission only
20.	Place, Time and Date of opening of Technical proposals received in response to the Bid Document notice	<b>29.10.2021 03:00 pm</b> IT Department, Worli Data Centre, Gr. Floor, Eng. Hub Bldg., Dr. E. Moses Road, Worli, Mumbai – 400018.
21.	Place, Time and Date of opening of Financial proposals received in response to the Bid Document notice	To be Informed Later
<b>E. Evaluation of Bids and Awarding of Contract</b>		
22.	Minimum Aggregate Technical Score	70 out of 100 points
23.	Signing of Contract Agreement with MCGM	Within 30 days after the issuance of letter of intent to the successful bidder

### 3.2 Purpose of the Bid Document

The purpose of this Bid Document is ***to Select a Service Provider for Implementation of IT Audit at MCGM*** as per the scope defined in the subsequent sections. This document provides information to enable the bidders to understand the broad requirements to submit their "Bids". The detailed scope of work is below in this bid document.

### **3.3 Cost of Bid Document**

The Cost of bid document as mentioned in the **Bid Data Sheet**

### **3.4 Bidder Registration and Instructions**

Before entering into online tendering process, the bidder should complete the registration process so as to get User ID for eProcurement system using URL <https://portal.mcgm.gov.in>

### **3.5 Bid Preparation Cost**

1. The Bidder is responsible for all costs incurred in connection with participation in this process, including, but not limited to, costs incurred in the conduct of informative and other diligence activities, participation in meetings/discussions/presentations, preparation of bid, in providing any additional information required by MCGM to

facilitate the evaluation process, and in negotiating a definitive Contract or all such activities related to the bid process. MCGM will in no case be responsible or liable for those costs, regardless of the conduct or outcome of the bidding process.

2. This bid does not commit MCGM to award a contract or to engage in negotiations. Further, no reimbursable cost may be incurred in anticipation of award. All materials submitted by the Bidder shall become the property of MCGM and may be returned at its sole discretion.

### 3.6 Pre-bid Meeting

1. MCGM will host a Pre-bid Meeting for queries (if any) by the prospective bidders. Details regarding the date, time and place of the meeting are provided in Section 3.1. The representatives of the bidders may attend the pre-bid meeting at their own cost. The purpose of the pre-bid meeting is to provide a forum to the bidders to clarify their doubts / seek clarification or additional information, necessary for them to submit their bid.
2. All enquiries from the bidders relating to this bid must be submitted to the designated contact person as mentioned in section 3.1 of this bid document. The queries should necessarily be submitted in the following format as an editable Microsoft Excel/Spreadsheet document along with PDF:

#	Bid Document Reference (Volume, Section No.)	Page Number	Content of the bid requiring clarification	Clarification Sought/Query
1				
2				
3				

3. Authorisation letter in the name of the person attending the pre-bid meeting needs to be submitted on the letterhead of the Bidder before start of the pre-bid meeting in the format specified in Annexure. The scanned, digitally signed authorization letter should be submitted via email on email id : [manager01.it@mcgm.gov.in](mailto:manager01.it@mcgm.gov.in)
4. Queries submitted post the specified deadline, or which do not adhere to the specified format may not be responded to. All the responses to the queries (clarifications / corrigendum) shall be made available on <https://portal.mcgm.gov.in>

### **3.7 Amendment of Bid Document**

1. At any time before the deadline for submission of bids, MCGM, may, for any reason, whether at its own initiative or in response to a clarification requested by a prospective Bidder, modify the bid document by an amendment. All the amendments made in the document would be published on <https://portal.mcgm.gov.in>.
2. The bidders are advised to visit the <https://portal.mcgm.gov.in> website on regular basis for checking necessary updates. MCGM also reserves the rights to amend the dates mentioned in this bid for bid process. It will be assumed that the amendments have been taken into account by the Bidder in its bid.
3. In order to afford prospective Bidders reasonable time in which to take the amendment into account in preparing their bids, MCGM may, at its discretion, extend the last date for the receipt of Bids.

### **3.8 Rights to Terminate the Process**

1. MCGM may terminate the bid process at any time and without assigning any reason. MCGM makes no commitments, express or implied, that this process will result in a business transaction with anyone.
2. This bid document does not constitute an offer by MCGM. The Bidder's participation in this process may result in MCGM selecting the Bidder to engage in further discussions and negotiations towards execution of a contract. The commencement of such negotiations does not, however, signify a commitment by MCGM to execute a contract or to continue negotiations. MCGM may terminate negotiations at any time without assigning any reason.

### **3.9 Earnest Money Deposit (EMD) and Refund**

1. Bidders shall pay, along with their Bids, EMD amount as mentioned in Bid Data Sheet, and it shall be paid online.
  2. In case a bid is submitted without the EMD as mentioned above then MCGM reserves the right to reject the bid without providing opportunity for any further correspondence to the Bidder concerned.
  3. The EMD shall be denominated in Indian Rupees only. No interest shall be paid by MCGM towards the deposited EMD.
-



4. EMD of the successful bidder will be discharged when the bidder has signed the agreement and furnished the required Security Deposit/PBG as per format. EMD of L-2 and other bidders shall be refunded immediately after opening of financial bid. In case, the successful bidder becomes non-responsive or successful bidder withdraws the bid or is unwilling to extend the bid validity period, in such circumstances, if L-2 bidder is agreeable to extend the bid validity period and ready to deposit the requisite amount of EMD to the department within the stipulated time period i.e. 15 days, the department will process further as per normal procedure.
5. The EMD may be forfeited in any of the following cases:
  - i. If a Bidder withdraws its bid or increases its quoted prices during the period of bid validity or its extended period, if any
  - ii. In the case of a successful Bidder, if the Bidder fails to sign the Contract or to furnish Bank Guarantee/Security Deposit within specified time in accordance with the format given in this bid document
  - iii. During the bid process, if a Bidder indulges in any such deliberate act as would jeopardize or unnecessarily delay the process of bid evaluation and finalization
  - iv. During the bid process, if any information is found wrong / manipulated / hidden in the bid.
6. The decision of MCGM regarding forfeiture of the EMD and rejection of bid shall be final and shall not be called upon question under any circumstances.
7. No rejections and forfeiture shall be done in case of curable defects. For non-curable defects the 10% of EMD shall be forfeited and bid will be liable for rejection.

Note:

1. Curable Defect shall mean shortfalls in submission such as:
  - a. Non-submission of following documents
    - i. Valid Registration Certificate
    - ii. Valid Bank Solvency
    - iii. GST Registration Certificate
    - iv. Certified Copies of PAN documents and photographs of individuals, owners, etc.

- v. Partnership Deed and any other documents
  - vi. Undertakings as mentioned in the tender document.
2. Non-curable Defect shall mean
- a. In-adequate submission of EMD/ASD amount,
  - b. In-adequacy of technical and financial capacity with respect to Eligibility criteria as stipulated in the tender.
  - c. Wrong calculation of Bid Capacity.
  - d. No proper submission of experience certificates and other documents, etc.

### **3.10 Solvency Certificate**

1. A valid Bank Solvency Certificate of amount as mentioned in the Bid Data Sheet has been issued not more than six months prior to the date of submission of bid needs to be submitted in the Pre-Qualification folder (Packet 'A').

### **3.11 Submission of Bids**

1. Complete bidding process will be online (e-Bidding) in two packet system. All the notification and details regarding terms and conditions related to this bid notice hereafter will be published online on web site.
2. Bidding documents can be seen, downloaded and submitted in electronic format on the MCGM website. The deadline for submission of bid is specified in the Bid Data Sheet of this document.
3. Technical bids will be opened as per the details found in the Bid Data Sheet of this document.
4. Bidder should submit information and scanned copies of all the documents in PDF format in Pre-Qualification folder (Packet 'A') as mentioned in the Bid Document.
5. Bidder may be requested to submit original documents for verification during evaluation of technical bids as and when required.
6. Time and date of opening of financial bid will be informed by email to technically qualified bidders.
7. An authorized representative of the Bidder should have valid class III Digital Signature Certificate (DSC) obtained from any Certifying Authority. The authorized representative of the Bidders shall digitally sign the original Technical bid and Commercial bid. The authorization shall be in the form of a written power of attorney

accompanying the bid or in any other form demonstrating that the representative has been duly authorized to sign.

8. On opening the Pre-Qualification folder, if it is found that the Bidder has not submitted required documents as per Pre-Qualification folder (Packet 'A') then the Bidder shall be intimated to comply with the said documents within 3 days from the intimation from MCGM (through email), otherwise they will be treated as non-responsive.
9. MCGM reserves the right to accept or reject any or all the Bids without assigning any reason. Moreover, if no intimation is provided by MCGM then the documents submitted cannot be deemed as accepted.

### **3.12 Process for Submission**

The procedure for quoting and uploading Tender Documents is available on <https://portal.mcgm.gov.in>

Before purchasing / downloading the tender copy, tenderer may refer to Pre-Qualification criteria.

The tenderer shall pay the EMD / Bid security through payment gateways before submission of Bid and shall upload the screenshot of receipt of payment in Packet 'A'

The e-tender is available , <https://portal.mcgm.gov.in>, as mentioned in Bid Data Sheet. The tenders duly filled in should be uploaded and submitted online on or before the end date of submission. The Packet ‘A’, and Packet ‘B’ of the tenderer will be opened as per the timetable mentioned in the Bid Data Sheet

The Municipal Commissioner reserves the right to reject all or any of the e-Tender(s) without assigning any reason at any stage. The dates and time for submission and opening the tenders are as mentioned in the Bid Data Sheet. If there are any changes in the dates the same will be displayed on <https://portal.mcgm.gov.in>

### **3.13 Site Visit**

1. Bidders are welcome to visit the site/s and obtain additional information at their own cost and responsibility. However, a prior appointment with the concerned officials is recommended.

### **3.14 Language of the Bid**

1. The Application and all related correspondence and documents in relation to the Bidding Process shall be in English language. Supporting documents and printed literature furnished by the Applicant with the Application may be in any other language provided that they are accompanied by translations of all the pertinent passages in the English language, duly authenticated and certified by the Applicant. Supporting materials, which are not translated into English, may not be considered. For the purpose of interpretation and evaluation of the Application, the English language translation shall prevail.

### **3.15 Bid Submission Format**

1. The entire bid shall strictly be as per the format specified in this RFP.

### **3.16 Documents Comprising the Bid**

1. Following table is provided as the guideline for submitting various important documents along with the bid.

#	Type of Packet	Documents to be uploaded
01	Pre-Qualification Folder (Packet A)	<ul style="list-style-type: none"> <li>✓ Cover Letter</li> <li>✓ Board Resolution authorizing the Bidder to sign/ execute the proposal as a binding document and also execute all relevant agreements forming part of Bid Document Or Power of Attorney executed by the Bidder in favor of the Principal Officer or the duly Authorized Representative, certifying him/her as an authorized signatory for the purpose of this Tender</li> <li>✓ Service Tax/GST Registration Copy</li> <li>✓ Income Tax Certificate (ITR) along with copy of PAN Card</li> <li>✓ Bidders' Particulars as per format given in Annexure I</li> <li>✓ Certified copy of Partnership Deed/Certified copy of Certificate of Incorporation/ Registration Certificate</li> <li>✓ Certificate of Cert-In empanelment</li> <li>✓ Valid Solvency Certificate</li> <li>✓ Copy of the audited balance sheet of the company for last three consecutive financial years (2017-18, 2018-19, 2019- 20)</li> <li>✓ Copy of the audited Profit &amp; Loss statements of the company for the last three consecutive financial years (2017-18, 2018-19, 2019- 20)</li> <li>✓ Detailed CVs of the resources to be deployed in the project</li> <li>✓ Copy of Work Order &amp; Work Completion / In-progress certificate of Systems Audit for SAP applications/ cloud security review/ IT Process Review/ System Integration Review/ IT Infrastructure Review/ Performance Review from the respective client of the bidder/ Self-Declaration duly signed by the signing authority</li> <li>✓ Declaration regarding blacklisting in the format given in Annexure I and Commercial in the format given in Annexure III</li> </ul>
02	Technical Proposal Folder (Packet B)	<ul style="list-style-type: none"> <li>✓ Technical Proposal in the format specified in Annexure II</li> <li>✓ Details of Manpower Resources Proposed</li> <li>✓ High Level Strategy Document highlighting approach on Systems Audit and IT Infrastructure Audit program</li> <li>✓ Other Documents (as per requirements of the Bid Document)</li> <li>✓ Commercial Bid Declaration</li> </ul>
03	Commercial Proposal Folder (C)	<ul style="list-style-type: none"> <li>✓ Commercial Bid (online)</li> <li>✓ Bidder shall mandatorily upload the information of applicable taxes on various items in the proforma as enclosed under “<b>Commercial Format (Online)</b>” in “C” packet.</li> </ul>

2. Bidders shall furnish the required information on their Pre-Qualification, technical and financial bids in enclosed formats only. Any deviations in format may make the bid liable for rejection. Disclosure of Commercial information of the bid in Pre-Qualification or Technical Envelope shall be sufficient grounds for rejection of the bid.
3. The bidders shall categorically provide their Email-ID in packet 'A'.

### **3.17 Evaluation Process**

1. The Bidder must possess the technical know-how and the financial wherewithal that would be required to successfully provide the services sought by MCGM, for the entire period of the contract. The bid must be complete in all respects, conform to all the requirements, terms and conditions and specifications as stipulated in the bid document.
2. The evaluation process of the bid proposed to be adopted by MCGM is indicated in this section. The purpose of this section is to provide the Bidder an idea of the evaluation process that MCGM may adopt.
3. MCGM shall appoint a Bid Evaluation Committee (BEC) to scrutinize and evaluate the technical and commercial bids received. The BEC will examine the Bids to determine whether they are complete, responsive and whether the bid format conforms to the bid requirements. MCGM may waive any informality or non-conformity in a bid which does not constitute a material deviation according to MCGM.
4. There should be no mention of bid prices in any part of the bid other than the Commercial Bid.

5. Any attempt by a bidder to influence the bid evaluation process may result in the rejection of Bid.

### **3.18 Opening of Bid**

1. All the bids received within the deadline shall be opened at the date, time and place.
2. The Bidder's representatives who are present shall be requested to sign the attendance sheet.
3. Authorization letter in the name of the person attending bid opening meeting needs to be submitted on the letterhead of the Bidder during bid opening in the format specified in the tender document.
4. Once the bids are opened each bid will be checked for pre-qualification criteria.

### **3.19 Evaluation of Technical Bid**

1. The Technical Bids of only those Bidders, who qualify in the Pre-Qualification stage, shall be considered and will be evaluated as per the evaluation criteria in this clause. The Bid Evaluation Committee (BEC) shall invite each Bidder to make a presentation-cum-demonstration as part of the technical evaluation.
2. The BEC may require verbal/written clarifications from the Bidders to clarify ambiguities and uncertainties arising out of the evaluation of the Bid documents (to be stated precisely as it should be in MCGM's interest).
3. In order to qualify technically, a Bid must secure a minimum of 70% of total marks in technical evaluation after summing up. Only those Bids which have a minimum score of 70% of total marks in technical evaluation will be considered for opening of their Commercial Bid. Only the Bids qualifying the technical evaluation will be considered for commercial evaluation.
4. MCGM reserves the right to lower the minimum required marks if none of the Bidders achieves 70% of the total marks.
5. Only the Bids qualifying the technical evaluation will be considered for commercial evaluation.
6. Technical Evaluation of the bids would be carried as follows:

#	Parameter	Marks
A	Financial Strength	10
B	Technical Competence	40
C	Quality of Manpower	27
D	Quality of Proposal	23
	<b>Total</b>	<b>100</b>

The 4 evaluation categories are further divided into various sub-categories (i.e. in Category A, B, C, D) as broadly mentioned below.

Section	Technical Evaluation Parameter	Point System	Max. Marks	Supporting
<b>Financial Strength</b>				
TQ_1	Financial ability of the bidder to execute similar large projects	Turnover for the last three financial years (2017-18, 2018-19, 2019-20) from Security Audit & Security Consulting Services. <ul style="list-style-type: none"> <li>• Turnover <math>\Rightarrow</math> 6 Cr and Turnover <math>\leq</math> 16.5 Cr = 7 marks</li> <li>• Turnover <math>&gt;</math> 16.5 Cr and Turnover <math>\leq</math> 26.5 Cr = 8.5 marks</li> <li>• Turnover <math>&gt;</math> 26.5 Cr = 10 marks</li> </ul>	10	Copy of the audited Balance Sheet and Profit & Loss Statement of the company and Certificate from the Chartered Accountant clearly stating the turnover and also mentioning turnover from work related to Security Audit & Security Consulting Services.
<b>Technical Competence</b>				



Section	Technical Evaluation Parameter	Point System	Max. Marks	Supporting
TQ_2	Experience of the bidder in implementing Systems Audit projects for SAP applications	<ul style="list-style-type: none"> <li>At least 3 projects = 7 marks</li> <li>At least 4 projects = 8.5 marks</li> <li>At least 5 projects = 10 marks</li> </ul>	10	<ul style="list-style-type: none"> <li>Copy of Work Order &amp; Work Completion certificate of the project from the client clearly depicting the scope of work, contract period and project value.</li> </ul>
TQ_3	Experience of the bidder in implementing Security audit for IT Infrastructure	<ul style="list-style-type: none"> <li>At least 3 projects = 7 marks</li> <li>At least 4 projects = 8.5 marks</li> <li>At least 5 projects = 10 marks</li> </ul>	10	
TQ_4	Experience of the bidder in implementing projects for Systems Audit projects for non-ERP applications	<ul style="list-style-type: none"> <li>At least 3 projects = 7 marks</li> <li>At least 4 projects = 8.5 marks</li> <li>At least 5 projects = 10 marks</li> </ul>	10	

Section	Technical Evaluation Parameter	Point System	Max. Marks	Supporting
TQ_5	Experience of the bidder in implementing projects for IT Process Review	<ul style="list-style-type: none"> <li>At least 3 projects = 7 marks</li> <li>At least 4 projects = 8.5 marks</li> <li>At least 5 projects = 10 marks</li> </ul>	10	
<b>Quality of Manpower</b>				
TQ_6	ISO27001 /ISO 27001 Lead Implementers/ Auditors	<ul style="list-style-type: none"> <li>At least 10 members = 3 marks</li> <li>&gt;10 members = 5 marks</li> </ul>	5	Certificate from HR Head of the company
TQ_7	CISA/CISM/CISSP certified	<ul style="list-style-type: none"> <li>At least 10 members = 3 marks</li> <li>&gt;10 members = 5 marks</li> </ul>	5	
TQ_8	OSCP/ CEH/GCIH/CCNA Certified professionals	<ul style="list-style-type: none"> <li>At least 10 members = 3 marks</li> <li>&gt;10 members = 5 marks</li> </ul>	5	
TQ_9	Quality of the IT Manpower Proposed for the project	<ul style="list-style-type: none"> <li></li> </ul>	12	Resume of one resource for each profile i.e. Project Manager, Senior Consultant and Junior Consultant

Section	Technical Evaluation Parameter	Point System	Max. Marks	Supporting
	Implementation & Support			<p>across the following three categories:</p> <ul style="list-style-type: none"> <li>• Systems Security Review</li> <li>• Security Review of IT Infrastructure</li> <li>• IT Process Review</li> </ul> <p>For each profile, MCGM would require copies of the education qualifications and professional certifications along with the complete resume as per the format specified in the bid document.</p>
<b>Quality of Proposal</b>				
TQ_7	Detailed understanding of the scope of project, approach & methodology, detailed project plan along with the timelines and resource deployment plan, understanding mitigation of risks.	<ul style="list-style-type: none"> <li>• Understanding of the project and approach &amp; methodology: 8 marks</li> <li>• Bidder's awareness of risks and mitigation in the project: 5 marks</li> </ul>	13	Qualitative assessment of the detailed project plan, project scope understanding and proposed resources deployment plan

Section	Technical Evaluation Parameter	Point System	Max. Marks	Supporting
TQ_8	Technical Presentation and clarifications / answers given to the BEC during presentation by the Bidder	<ul style="list-style-type: none"> <li>The Bidder shall prepare a presentation regarding the technical bid. The BEC shall evaluate the presentation based on the following criteria:</li> <li>Understanding demonstrated regarding the project scope: 2 marks</li> <li>Approach &amp; methodology to meet the project requirements: 4 marks</li> <li>Quality of response against queries raised by the committee: 4 marks</li> </ul>	10	Presentation and responses.
<b>Total Marks</b>			<b>100</b>	

All the bidders satisfying the above-mentioned parameters with respect to minimum value will be declared technically qualified.

### **3.20 Opening of Commercial Bid**

1. The Commercial bids shall not be opened by MCGM until the evaluations of the Technical Bids have been completed.
2. After the technical evaluation is completed and MCGM has issued its no objection (if applicable), MCGM shall notify those Bidders whose proposals did not pass the technical evaluation or were considered as non-responsive to the Bid Document and scope of work, that their Financial Proposals will not be opened. Only those Bids which have a minimum score of 70% of total marks in technical evaluation will be considered for opening of their Commercial Bid.
3. MCGM shall simultaneously notify in writing to bidders who have cleared the technical evaluation, the date, time and location for opening the Financial Proposals. The opening date would allow Bidders sufficient time to make arrangements for attending the opening. Bidders' attendance at the opening of Financial Proposals is optional.
4. MCGM shall prepare a record of the bid opening that shall include, at a minimum: the name of the Bidder and the bid Price, and any other details as MCGM may consider appropriate. The Bidders' representatives who are present shall be requested to sign the attendance sheet. A copy of the record shall be distributed to all Bidders.
5. Financial Proposals shall be opened publicly in the presence of the Technically Qualified Bidders' representatives who choose to attend. The name of the Technically Qualified Bidders shall be read aloud.
6. Commercial Bids from bidders who have failed to qualify in evaluation of the technical bid will not be opened.
7. Only bids that are opened and read out at the bid opening shall be considered further.
8. Authorization letter in the name of the person attending bid opening needs to be submitted on the letterhead of the Bidder during bid opening in the format specified in the bid document.

9. The Commercial Bids will be evaluated by MCGM for completeness and accuracy. Arithmetical errors will be rectified on the following basis. If there is a discrepancy between the unit price and the total price that is obtained by multiplying the unit price and quantity, the unit price shall prevail, and the total price shall be corrected. If there is a discrepancy between words and figures, the amount in words will prevail.
10. The amount stated in the proposal form, adjusted in accordance with the above-mentioned procedure, shall be considered as binding, unless it causes the overall proposal price to rise, in which case the proposal price shall govern.
11. If the bidder does not accept the correction of errors, its bid will be rejected, and the bid security may be forfeited.
12. Activities and items described in the Technical Proposal but not priced, shall be assumed to be included in the prices of other activities or items. In case an activity or line item is quantified in the Financial Proposal differently from the Technical Proposal, the Evaluation Committee shall correct the quantification indicated in the Financial Proposal so as to make it consistent with that indicated in the Technical Proposal, apply the relevant unit price included in the Financial Proposal to the corrected quantity and correct the total Proposal cost.

### **3.21 Selection Method**

1. The technically qualified bidder with lowest total cost (L1) rate shall be automatically selected.
2. All rights regarding selection of agency will reside with MCGM.

### **3.22 Right to Accept or Reject Any or All Bids**

Notwithstanding anything contained in this Tender, MCGM reserves the right to accept or reject any Application and to annul the Bidding Process and reject all Applications/ Bids, at any time without any liability or any obligation for such acceptance, rejection or annulment, and without assigning any reasons therefore. In the event that the Authority rejects or annuls all the Bids, it may, in its discretion, invite all eligible Bidders to submit fresh Bids hereunder.

MCGM reserves the right to reject any Application and/ or Bid if:

- a) At any time, a misrepresentation is made or uncovered, or
- b) The bidder does not provide, within the time specified by the Authority, the supplemental information sought by the Authority for evaluation of the Application.

In case it is found during the evaluation or at any time before signing of the Agreement or after its execution and during the period of subsistence thereof including the concession thereby granted by MCGM, that one or more of the pre-qualification conditions have not been met by the Bidder, or the Bidder has made any misrepresentation or has given any incorrect or false information, the Bidder shall be disqualified forthwith if not yet appointed as the Successful Bidder either by issue of the LOA (Letter of Approval/Acceptance) or entering into of the Agreement, and if the Bidder has already been issued the LOA or has entered into the Concession Agreement, as the case may be, the same shall, notwithstanding anything to the contrary contained therein or in this TENDER, be liable to be terminated, by a communication in writing by MCGM to the Bidder, without Bidder being liable in any manner whatsoever to the Bidder and without prejudice to any other right or remedy which MCGM may have under this TENDER, the Bidding Documents, the Concession Agreement or under applicable law. MCGM reserves the right to verify all statements, information and documents submitted by the Bidder in response to the TENDER. Any such verification or lack of such verification by MCGM shall not relieve Bidder of its obligations or liabilities hereunder nor will it affect any rights of MCGM there under.

The bid shall be rejected if the bidder-

- a) Stipulates the validity period less than 180 days.
- b) Stipulates own condition/conditions.
- c) Bid not fill and (digital) sign undertaking forms, which are incorporated, in the document.

### **3.23 Notification of Award and Signing of Contract**

1. Prior to the expiration of the period of bid validity, the Bidder will be notified in writing email that their bid has been accepted.

2. At the time MCGM notifies the successful Bidder that its bid has been accepted, MCGM will send the Bidders the proforma for Contract, incorporating all clauses/agreements between the parties. The successful Bidder shall sign and date the Contract and return it to MCGM. Draft Format of the contract has been included in the bid document.

### **3.24 Security Deposit (Bank Guarantee)**

1. The Bidder shall at his own expense, deposit with Corporation, within Thirty (30) working days of the notification of award of the contract an unconditional and irrevocable Bank Guarantee (BG) from the list of approved banks (specified in the bid document) as per the format given in this bid, payable on demand, for the due performance and fulfilment of the contract by the Bidder.
2. This Bank Guarantee will be for an amount equivalent to 10% of the total contract value. All charges whatsoever such as premium, commission, etc. with respect to the Bank Guarantee shall be borne by the Bidder.
3. Details on validity of the bank guarantee are specified under section 3.1 of this document. The Bank Guarantee letter format can be found in this document.
4. The Bank Guarantee may be discharged/ returned by Corporation after contract period upon being satisfied that there has been due performance of the obligations of the Bidder under the contract. However, no interest shall be payable on the Bank Guarantee.
5. In the event of the Bidder being unable to service the contract for whatever reason, MCGM would invoke the BG. Notwithstanding and without prejudice to any rights whatsoever of MCGM under the Contract in the matter, the proceeds of the BG shall be payable to MCGM as compensation for any loss resulting from the Bidder's failure to complete its obligations under the Contract. MCGM shall notify the Bidder in writing of the exercise of its right to receive such compensation within 14 days, indicating the contractual obligation(s) for which the Bidder is in default.
6. The 30 days notice period shall be considered as the 'Cure Period' to facilitate the Selected Agency to cure the breach. The BG shall be evoked only if the breach is solely attributable to the bidder and the bidder fails to rectify the breach within the 'Cure Period'.
7. MCGM shall also be entitled to make recoveries from the Bidder's bills, bank guarantee, or from any other amount due to the Bidder, the equivalent value of any payment made to the Bidder due to inadvertence, error, collusion, misconstruction or misstatement.



8. If Security deposit / Bank guarantee is not submitted within the stipulated period, EMD will be forfeited.

### 3.25 Failure to agree with the Terms and Conditions of the Bid/Contract

1. Failure of the Bidder to agree with the Terms and Conditions of the bid/Contract shall constitute sufficient grounds for the annulment of the award of contract, in which event the contract may be awarded to the next most responsive Bidder (i.e. L2 Bidder).
2. In such a case, MCGM shall invoke the BG of the L1 Bidder.
3. All required documents for execution of the contract shall be submitted within 30 days from the date of issue of letter of acceptance. If the documents are not submitted within the stipulated time a penalty of Rs 5000/- per day will be applicable to the contractor. All contract documents need to be duly affixed with stamp duty properly signed along with evidence/proof of payment of security/contract deposit/within 30 days from the date of letter of acceptance received by him.

### 3.26 Terms and Conditions of the Bid

1. Bidder is required to refer to the draft Contract Agreement, provided in this bid, for all the terms and conditions (including project timelines) to be adhered by the successful Bidder during Project Implementation and Post implementation period. Please note that one needs to read the Contract Agreement as a whole document; and the Annexure mentioned there-in may not correspond to the bid Annexure. Please refer to the Interpretation Section of the Agreement (Section 2 of draft agreement) for reference in the Annexure of this tender document.

### 3.27 Legal and Stationery Charges

The successful Bidder will have to bear the legal & stationery charges as below:

❖ Contract Value						Legal+ Stationery Charges (₹)
From	₹.	0	To	₹.	50,000/-	Nil
From	₹.	50,001/-	To	₹.	1,00,000/-	5710/-
From	₹.	1,00,001/-	To	₹.	3,00,000/-	9,430/-
From	₹.	3,00,001/-	To	₹.	5,00,000/-	11,330/-
From	₹.	5,00,001/-	To	₹.	10,00,000/-	13,190/-
From	₹.	10,00,001/-	To	₹.	20,00,000/-	15,060/-
From	₹.	20,00,001/-	To	₹.	40,00,000/-	16,960/-
From	₹.	40,00,001/-	To	₹.	1,00,00,000/-	18,830/-
From	₹.	1,00,00,001/-	To	₹.	10,00,00,000/-	22,220/-
From	₹.	10,00,00,001/-	To	₹.	20,00,00,000/-	25,650/-

From	₹.	20,00,00,001/-	To	₹.	30,00,00,000/-	29,070/-
From	₹.	30,00,00,001/-	To	₹.	40,00,00,000/-	32,490/-
From	₹.	40,00,00,001/-	To	₹.	50,00,00,000/-	35,880/-
From	₹.	50,00,00,001/-	To	₹.	1,00,00,00,000/-	42,720/-
From	₹.	1,00,00,00,001/-	To	₹.	2,00,00,00,000/-	52,970/-
From	₹.	2,00,00,00,001/-	To	₹.	3,00,00,00,000/-	59,790/-
From	₹.	3,00,00,00,001/-	To	₹.	4,00,00,00,000/-	68,290/-
From	₹.	4,00,00,00,001/-	To	₹.	5,00,00,00,000/-	76,820/-
from	₹.	5,00,00,00,001/-	To	₹.	Any amount	85,380/-(Maximum)

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

### 3.28 Stamp Duty

1. The stamp duty payable for the contract and BG shall be borne by the Implementation Agency IN WITNESS whereof the parties hereto have signed this on the day, month and year written as part of the agreement.
2. As per the provision made in Article 63, Schedule I of Bombay Stamp Act 1958, stamp duty is payable for “works contract” that is to say, a contract for works and labour or services involving transfer of property in goods (whether as goods or in some other form) in its execution and includes a sub-contract, as under:

Contract Value	Stamp Duty
Up to Rs. 10,00,000/-	Rs. 500/-
From Rs. 10,00,001/- To Any Limit	Rs. 500/- plus 0.1% of the amount above Rs. 10,00,000 (Subject to Maximum Rs. 25,00,000/-)
Stamp Duty on BG	0.5% for the amount secured by BG subject to maximum of Rs. 25,00,000/-.

3. The successful Bidder shall enter into a contract agreement with MCGM within 30 days from the date of issue of LOA and the same should be adjudicated for payment of Stamp Duty by the successful Bidder. A successful Bidder should submit certificate from Chartered Accountant regarding GST.
4. Further shortfall if any, in amount of stamp duty paid as against prescribed amount for the documents executed in Mumbai City and Mumbai Suburban District be recovered from the concerned work contractors and to deposit the deficit or unpaid Stamp Duty and penalty by two separate Demand Draft or Pay Order in favour of “Superintendent of Stamp, Mumbai” within 15 days from intimation thereof.

5. All legal charges and incidental expenses in this respect shall be borne and paid by the successful Bidder.

## **4 Scope of Work**

### **4.1 Introduction**

The Service Provider shall be responsible for the following:

- Conduction of IT Infrastructure Security Audit
- Conduction of SAP Applications Audit
- Conduction of Non - SAP Application Audit
- Conduction of location-based Audit

Overall Scope of Work will be divided in 2 sections as mentioned below:

- Preliminary Review
- Compliance Review

### **4.2 Preliminary Review**

#### **4.2.1 IT Infrastructure Audit of WDC**

##### **4.2.1.1 IT Infrastructure review of DC**

It involves review of entire IT operations for MCGM's Worli Data Center for internal applications. This includes review of asset management, capacity management, physical and logical access, etc. This would also include physical visits to Data Center and audit of the power, cooling, access controls, security, etc. This would include but not limited to analysis of following:

- Audit of physical and environmental security
- Complete review of hardware and software components
- DR plan review

##### **4.2.1.2 IT infrastructure in DC**

The scope of work for IT infrastructure audit of DC includes following, but not limited to:

- a. To study data center / disaster recovery center civil and interiors as per submitted layout
- b. To conduct a thorough examination of the physical environment in which all network devices and servers reside.
- c. To review the adequacy of server space in view of future requirement
- d. To review the access control facility
- e. To review the fire detection and prevention mechanism
- f. To review the fire protection system for server rooms
- g. To review the very early smoke detection systems for server rooms
- h. To review the water leak detection systems for server rooms
- i. To review the electrical subsystem (main panel, cables, Power Distribution Unit (PDU) and earthing)
- j. To review of Electrical Power requirement and availability.

- k. To review the UPS systems
- l. To review the availability of DG sets and control of fuel
- m. To review the precision (computer room standard) Air-conditioning systems for server room
- n. To review the closed-circuit television system (CCTV) area for monitoring entry/exit points and strategic locations within the server room
- o. To review the structured cabling system for functional areas as per layout
- p. To review the environmental threat protection (Air Purifier, Humidity Control etc.)
- q. To review operator awareness of physical security breaches
- r. To review safeguards to mitigate risks associated with earthquake and water related threats
- s. To verify the physical security policy and review of authorization documentation on file for everyone who has access to the Data Centre

#### 4.2.1.3 Network Architecture & Performance review

The audit is focused on the overall alignment and orchestration of the entire IT network of MCGM. This would include but not limited to analysis of following:

- Network segmentation
- Physical and logical separation of the networks
- Network Redundancy
- Egress and ingress points

#### 4.2.1.4 Security Review of Network Architecture

The scope of work for audit of network architecture includes the following, but not limited to:

- a. To study the network diagrams and understand the traffic flow in the network
- b. To study the as-is network segmentation
- c. To review and assess network topology, infrastructure hardware, Internet connections, network protocols in use and existing security solutions
- d. To identify logical/physical network inconsistencies
- e. To identify network utilization, bottlenecks and performance issues
- f. To study the security mechanisms between DMZ and internal network, and DMZ and Internet
- g. To review the network tools deployed in the network
- h. To review the utilization of IP Address space, IP conflict and dynamic/static IP address
- i. To recommend, if required, enhancements to the network design

Network Architecture review should be carried out for security and performance which include the following:

- Review the appropriate segregation of network into various trusted zones
- Review of network controls
- Review of security of network services
- Review the traffic flow in the network
- Review the existing routing/firewall/other network policies
- Review the route path and table audit

- Review of routing protocols and security controls therein
- Review the security measures at the entry and exit points of the network
- Obtaining information about the architecture and address scheme of the network
- Checking Inter-VLAN Routing and Optimization.
- Checking of redundancy configurations if any
- Routing Protocol Analysis
- Analyse protocols used and provide recommendation for improvement
- Analysis of load balancing mechanism
- Analysis of latency in traffic across various links
- Review placement of firewalls and DMZ's
- Review access control documentation and configuration
- Review logical access to business-critical applications, OS, database, network, physical access

A draft report highlighting the gaps observed and detailed recommendations should be prepared and discussed with the management. Upon discussion, approved management comments and target date of closure for the observations should be captured from the management.

#### 4.2.1.5 Vulnerability Assessment

MCGM expects an authenticated type but non-destructive vulnerability assessment to be carried out. Vendor should be able to cover a broad range of systems like operating systems, databases, web servers, application servers, network devices, security devices, etc. Vendors are expected to conduct the audit against the standard configuration and also as per the latest global standards and industry best practices. In case, any new asset is identified during project execution, vendor is expected to develop the checklist and conduct the assessment.

The purpose of the vulnerability assessment is to discover all systems on perimeter network or internet facing and to assess these systems for securities vulnerabilities. Vulnerability assessment shall attempt to determine vulnerabilities that may enable unauthorized logical access to protected system via the external network interfaces by a 'naive' intruder who has limited and/ or no previous knowledge of the MCGM's network. The vendor shall conduct vulnerability assessment against network and security infrastructure components to identify services in use and potential vulnerabilities present.

The assessment should check for various categories of threats including:

- a. Unauthorized access into the network and extent of such access possible
- b. Unauthorized modifications to the network and traffic flowing over network
- c. Extent of information disclosure from the network
- d. Spoofing of identity over the network
- e. Possibility of denial of services
- f. Possible threats from malicious codes (viruses and worms etc.)

- g. Possibility of traffic route poisoning

#### 4.2.1.6 Server Vulnerability Assessment / Operating System Audit

The server vulnerability assessment / operating systems audit would include the following, but not limited to:

- a. Vulnerability assessment of servers
- b. Secured operating system installation
- c. Patch and service pack levels for the operating systems as applicable
- d. Users and groups created, including user management, password complexity, etc.
- e. File system security of the OS (to include file integrity checks in addition to access control)
- f. Access rights and privileges
- g. Services and ports accessible
- h. Change management in terms of modification to the operating system
- i. Backup and emergency response measures
- j. Create baseline of critical parameters of the servers and OS configuration
- k. Determine anti-virus configurations, architecture, definition dates, scanning and updating policies.

#### 4.2.1.7 Vulnerability Assessment of Network Devices

The vulnerability assessment of network devices would include the following, but not limited to:

- a. To perform a comprehensive scan of all IP address ranges in use to determine what vulnerabilities exist in the network devices and servers, and to review all responses to determine if any risks exist.
- b. To use vulnerability scanners to scan the network devices and servers to determine if any vulnerabilities exist
- c. To search for back door traps in the Operating Systems
- d. To check for the known vulnerabilities in the Operating Systems, and applications like Browser, E-Mail, Web Server, Web Application Server, and FTP etc.
- e. To use tools to perform a password scan to determine accounts that have passwords that are "easy" to crack.
- f. To test for the presence of unnecessary services/applications those are running on the network devices/servers/workstations.

#### 4.2.1.8 Penetration Testing

The objective of the assessment is to determine the effectiveness of the security of organization's infrastructure and its ability to withstand an intrusion attempt. This may be achieved by conducting a comprehensive penetration test. The security assessment should use the industry standard penetration test methodologies (like OSSTM) and scanning techniques and will focus on applications.

The scope for penetration testing should include but not limited to list of internet facing websites/ applications. It is explicit that penetration tester should conduct vulnerabilities assessment consulting with concerned personnel and proper permission of MCGM. Finally, remediation and recommendations must be provided along with all findings.

Penetration testing should include the following, but not limited to:

- a. Network Security
  - i. Password Security Testing
  - ii. Router Security Assessment
  - iii. Anti-Virus System Security Assessment and Management Strategy
  - iv. Internet User Security
- b. Host Security
  - i. Unix/Linux System Security Assessment
  - ii. Windows System Security Assessment
  - iii. Web Server Security Assessment
  - iv. Other relevant/mapped application Security Assessment

#### 4.2.1.9 Network & Security Configuration Review

The bidder shall review the data center and wide area network of MCGM to identify single point of failures, network availability, logical segregation and deployment of security products/technologies etc. The assessment is to be carried out for Data Centre LAN, DR LAN, network connectivity from MCGM Bhavan and other offices to Data Centre, nodal site offices networks, etc.

The review is focused on the overall network and security management for MCGM. This would include but not limited to analysis of following:

- Firewall / VPN Audit
- Audit of Routers
- Network cabling
- Total bandwidth utilization
- Current network and security posture of the LAN / WAN architecture
- Network bottlenecks and performance issues
- Desktop Security Audit
- Virus / malware presence in network

#### 4.2.1.10 Audit of Security Devices

The audit shall encompass all the security devices (e.g. Firewall, VPN, etc.). The audit of security devices should include the following, but not limited to:



- a. Check for default configuration of the Firewall/ Switches
- b. Response to various protocols like TCP, UDP, ICMP, etc.
- c. List of open ports available for external users
- d. Verify rule sets for admin access, lockdown rule, internal user,
- e. External user, web server access, pop access to mail server, access to ICQ connections
- f. Audit of DMZ configuration
- g. VPN configuration access
- h. VPN access controls
- i. System authentication
- j. Insecure dynamic routing configuration
- k. Insecure service configuration
- l. Insecure TCP/IP Parameters
- m. Unnecessary services
- n. Remote login settings
- o. Latest software version and patches
- p. Logging
- q. Log functions viz. file location, Integrity and confidentiality of logs, Log analysis and rotation
- r. Audit of authentication mechanism (if used)
- s. Audit of encryption method (if used)
- t. Third party software used with firewall for additional services
- u. Firewall failure mode – fail open or fail secure
- v. Ease of recovery and backup of firewall

#### 4.2.1.11 Audit of Network Devices

The audit shall encompass all the network devices (e.g. routers, switches, etc.). The audit of network devices should include the following, but not limited to:

- a. To review and assess all router configurations like version, access control lists, password configuration, miscellaneous protocol configurations, logging and configurations to prevent common internet attacks
- b. To review the configuration of switches and check for configuration access
- c. Verify access control lists
- d. Check for unnecessary services & protocols
- e. To conduct routing table overview
- f. To review router memory and CPU utilization
- g. To conduct router error analysis
- h. To review broadcast errors
- i. To review router retransmissions
- j. To review port security, IP filtering features of switches
- k. To review login banners of routers / switches
- l. Audit logs

- m. Log functions viz. file location, integrity and confidentiality of logs, log analysis, and log rotation.
- n. Suggest standard practice for storing logs
- o. Audit of existing backup solution & video conferencing units

Review the configuration of switches based on following security controls:

- User authentication and password management
- Authentication, authorization and account settings
- Security settings on different management interfaces (physical and logical)
- SNMP configuration
- Access controls
- Use of logging and monitoring
- Configuration to defy common security attacks like IP spoofing, ICMP redirects
- Delegation of privileged use in accordance with job function
- Session management
- Configuration of VLANs and associated protocol
- Security Controls around port security, Spanning Tree protocol, VLAN Trunking protocol etc
- Updated version of IOS / patches
- Remote login settings
- Unnecessary services

Review the configuration of routers based on following security controls:

- User authentication and password management
- Authentication, authorization and account settings
- Security settings on different management interfaces (physical and logical)
- SNMP configuration
- Use of logging and monitoring
- Configuration to defy common security attacks like IP spoofing, ICMP redirects
- Delegation of privileged use in accordance with job function
- Routing protocols configured and appropriate security settings
- Review of access lists for different network segments (to different outside networks)

- Remote login settings
- Updated version of IOS / patches
- Unnecessary services

Review the configuration parameters and rule base of the firewall(s) which include the following controls:

- Placement of firewall within the network
- Policies and rule sets
- Authentication, Authorization and accounting
- Auditing, logging, monitoring, alerting mechanism
- Password control and security controls for administrative / management interfaces
- Configuration to defy commonly known security attacks
- Configuration of access control and priority of traffic flow
- Allowed inbound and outbound services
- Service proxies, circuit-level gateways, and packet filters
- Surrounding firewall security issues
- Domain name services
- Router protection and participation in firewall functionality
- VPN configuration and encryption
- Updated version of OS / patches

Review the configurations for the proxy server including following controls:

- Types and applicability of interfaces configured
- Allowed / Denied range of hosts
- Review of internal and external interfaces
- Access controls and allocation of privileges
- Authentication mechanism

#### 4.2.1.12 Server/OS Audit

The server/ OS configuration audit should include the following, but not limited to:

- a. File system security
- b. Account Policies
- c. Access Control
- d. Network Settings / Network Port / Network Access Details

- e. System Authentication
- f. Logging and auditing
- g. Patches and updates
- h. Unnecessary services
- i. Remote login settings

#### 4.2.1.13 Infrastructure Hardware Audit

The Infrastructure Hardware audit should include the following, but not limited to:

- a. Check server, network devices, backup devices hardware for out of support / out of life
- b. Check server virtualization (VMWare or other virtualization) software for out of support / out of life
- c. Check Patches and updates for server virtualization (VMWare or virtualization) software
- d. Access Control for virtualization (VMWare or other virtualization) software
- e. Detailed configuration parameters and secure hardening guidelines of Virtualization on the physical host.

#### 4.2.2 Email Security Audit

Confidentiality & Integrity are important aspects for business email solution. Email security should be a top priority as the email can contain sensitive data, such as upcoming business plans, or forecasts as well as personal information on customers / employees.

Email security audit would encompass the following, but not limited to:

- a. Risk assessment
- b. Threat and vulnerability analysis
- c. Email content and attachment filtering
- d. Email restrictions
- e. Attachment restrictions
- f. Log retention
- g. Email encryption
- h. Email server configurations
- i. Email anti- spoofing etc.

Email security audit would also cover review of email policy, email retention/backup/storage policy and account management review. The objective of E-mail security audit is to ensure that MCGM has a secure and well-governed email solution.

#### 4.2.3 Digital Forensics Readiness Assessment

This review is to be conducted to assess the capability of an organization to be able to collect, preserve, protect and analyze digital evidence so that this evidence can be effectively used in any legal matters, in disciplinary matters, in an employment tribunal or court of law.

The bidder shall conduct the digital forensic readiness assessment on the capability of the existing processes and technology implementation in tracking and tracing the incident at a faster rate along with a focus on reducing the business downtime, impact of cyber-attack, cost of investigation.

The bidder should assess the readiness of digital forensics covering the guidelines mentioned below, but not limited to:

- a. Existing log collection & retention policies of critical business applications, Firewall, IPS, router, load balancer, SIEM tools etc.
- b. Cyber Security Incident Response policy & framework
- c. Legal & regulatory compliance requirements
- d. Effectiveness of log monitoring & analysis
- e. Assess whether footprint of every activity is logged
- f. Assess the ability to recreate the incident in order to zero in the root cause
- g. Effectiveness of existing controls in detection, prevention of attacks
- h. Effectiveness of incident response such as handling, coordination & resolution
- i. Effectiveness of evidence preservation, collection
- j. Gap analysis for existing vs Standards such as ISO 27037, 27041, 27042, 27043, 27001.
- k. Recommend framework, policy, procedures for Digital Forensic readiness
- l. Recommend enhancements to existing process & technology to support forensic readiness

#### **4.2.4 Cloud Security Review**

The security controls review should comprise of the following:

- Review of Configuration Review of Cloud Servers (SAP + Non-SAP systems)
- Configuration Review of Cloud Integrated AD Server (AD is hosted at MCGM inhouse WDC)
- Security Review for Cloud Infrastructure, Cloud Platform, Cloud API
- Review of Anti-virus and other security components installed on the virtual machines.
- Detailed review and technical assessment of the virtualization systems.
- Detailed assessment of the physical host/servers on which the vms are created.
- Review for Cloud integrated services and managed services provided by the present cloud service provider
- Security review as per OWASP Top 10
- Detailed process review and certifications of the cloud service provider.
- Review of documentation and agreement contract between MCGM and cloud service provider.

- All the parameters as mentioned as a part of IT Infrastructure Audit will be applicable for Cloud vendors review as well.
- If in case during the audit period if MCGM moves the cloud infrastructure to other cloud services, the bidder must conduct the complete audit and assessment on the new cloud services accordingly. Also, the auditor need to review the migration process and suggest the gaps in the migration strategy.

#### **4.2.5 Process Review**

This review should be done to verify if the process around IT general controls (ITGC) are as per the industry best practices. The processes involve change management, incident management, user management, etc. The review involves test of design as well of the test of effectiveness.

Comprehensive “Design” and “Effectiveness” testing for the following process universe:

- Process Governance and Framework
- Application Management and Security Controls
- Identity and Access Management
- Change and Release Management
- Incident Management
- Backup Management and Disaster Recovery

##### **4.2.5.1 Audit overall IT operations as per ISO 27001 framework**

The following major activities have to be performed, but not limited to:

- a. Establish ISMS scope and IS objectives
- b. Perform gap assessment on existing security processes as per ISO/IEC 27001:2013 and prepare gap assessment report
- c. Assess the existing mandatory ISO/IEC 27001:2013 ISMS documents and perform gap assessment and enhance the policy documents to meet the certification requirements
- d. Develop statement of applicability for all the data centers. Identify the controls that are relevant and document the controls why it is not relevant with explanation
- e. Provide the required ISO/IEC 27001:2013 training and create awareness amongst relevant stakeholders
- f. Propose implementation of new or upgrading of existing security controls as per MCGMs’ business and ISO/IEC 27001:2013 ISMS requirements
- g. Assist MCGM’s security and operation team to deploy the security controls
- h. Monitor the security controls and identify the non-conformities
- i. Document the non-conformities and assign the owner and track it for closure
- j. Participate with MCGM for conducting internal ISMS audit during this engagement
- k. Assist MCGM- Information Security team for taking corrective actions and closure of non-conformities (if any);

- l. Assist MCGM-Information Security team in conducting management review of the ISMS;
- m. Support MCGM-Information Security team during certification audits (the Pre-certification audit and both Stage-I and Stage-II certification audits)
- n. Partner will procure following documents to perform the assessment and MCGM will own these documents for their continual security control review
- o. ISO/IEC 27001:2013 – Requirements
- p. ISO/IEC 27002:2013 - Security techniques: Code of Practice for IS controls

#### 4.2.5.2 Authorization and Segregation of Duties Controls

Testing of authorization and Segregation of duties should follow the guidelines mentioned below, but not limited to:

- a. Understand how system entitlements are used to enforce segregation of duties or authorized transactions.
- b. Perform sample testing of user application entitlement to ensure access to enter, approve, and/or modify transactions, data, or system configurations is restricted to authorized personnel (in a test environment).
- c. Populate issue and findings log with the gaps / deviations / issues noted (if any)

#### 4.2.5.3 Assessment of Role based Security for Applications under scope

Testing of role-based security should follow the guidelines covering mentioned below, but not limited to:

- a. Review of user creation/modification/deletion/maintenance procedures for the in-scope applications
- b. Review of privileged access rights granted to application, system administrators, service providers and vendors
- c. Assess the process for review of user logs for administrator and system users
- d. Review ongoing monitoring of effectiveness of implemented procedures and controls
- e. Review of account and password policy including controls such as
  - Users are assigned unique accounts
  - Adequate passwords are maintained e.g. alphanumeric, minimum number of characters, etc.
  - Periodic password changes and preventing repeated use of passwords
  - Review of implementation of password policy at system and application levels
- f. Account lockout policy for disabling user accounts after limited number of unsuccessful login attempts
- g. Segregation of duties controls /maker-checker controls through appropriate design and implementation of user roles/ profiles.
- h. Understand how system entitlements are used to enforce segregation of duties or authorized transactions.

- i. Understand how unsuccessful access attempts to applications in scope are logged and monitored
- j. Review the implementation and effectiveness of user access management in applications in the event of leaves.
- k. Review the segregation of development, production and test environments of applications

#### 4.2.5.4 Organizational Policies and Procedures:

The policies and procedures review should consist of the following activities:

- Policies for information security
- Review of the policies for information security
- Information security roles and responsibilities
- Segregation of duties
- Contact with authorities
- Contact with special interest groups
- Information security in project management
- Mobile device policy and teleworking
- Information transfer policies and procedures
- Agreements on information transfer
- Electronic messaging
- Confidentiality or nondisclosure agreements
- Capacity Management process
- Review of Documented operating procedures
- Review of Information systems audit controls
- HR Security Policy
- Business continuity and disaster recovery policy
- Vendor and third-party policy
- Physical and environmental Security management
- Other controls as applicable
- Training and awareness programs for Information security

IT process review is a vital part of any information security audit. The review should be conducted in the following areas to verify the adherence to IT processes during IT management:

#### 4.2.5.5 Change Management

Review of change management process should comprise of the following:



- Policy and procedure for change management
- Adherence to documented change management process
- Inventory of changes made to the infrastructure
- Change request tickets initiated for such changes
- Approval matrix for authorising the changes
- Impact analysis of the changes
- Testing results for the changes
- Approval for releasing the change in the production
- Other controls as applicable

#### 4.2.5.6 Incident Management

Review of incident management process should comprise of the following:

- Policy and procedure and responsibilities for incident management
- Adherence to documented incident management process
- Complaint logging mechanism
- Reporting information security events
- Reporting information security weaknesses
- Assessment of and decision on information security events
- Response to information security incidents
- Learning from information security incidents
- Collection of evidence
- Review the incident tickets as per the sampling methodology defined
- Setting up the priority
- Escalation mechanism
- Monitoring and reporting for parameters such as Incident response time, resolution time, etc.
- Other controls as applicable

#### 4.2.5.7 Asset Management

Review of asset (hardware/software) management process should comprise of the following:

- Policy and procedure for asset management including guidelines for acquisition of new IT equipment's/systems
- Adherence to documented asset management process
- Maintenance/Updating of asset registers

- Classification of information
- Labelling of information
- Handling of assets
- Inventory of assets
- Ownership of assets
- Acceptable use of assets
- Return of assets
- Management of removable media
- Disposal of media
- Physical media transfer
- Other controls as applicable

#### 4.2.5.8 Third Party management

Review of third-party management process should comprise of the following:

- Information security policy for supplier relationships
- Addressing security within supplier agreements
- Information and communication technology supply chain
- Monitoring and review of supplier services
- Managing changes to supplier services
- Verify existence of contracts with current IT service providers for IT contractors, hardware and software maintenance, networks, telephony, etc.
- Review the contracts for key parameters such as presence of minimum required service levels, key performance indicators (KPIs), penalties for KPI violations, etc.
- Policy and procedure for SLA monitoring
- Review SLA monitoring and reporting as per the sampling methodology defined
- Other controls as applicable

#### 4.2.5.9 System and Application Access management

Review of system and application access management should comprise of the following:

- Access control policy
- Access to networks and network services
- Information access restriction
- Secure log-on procedures
- Password management system
- Use of privileged utility programs

- Access control to program source code
- Other controls as applicable

#### 4.2.5.10 User access management

Review of user access management should comprise of the following:

- Policies and procedures for account management, end user sPecurity policy and user access management
- Review of list of users and corresponding user access request form as per the sampling methodology
- Review of user access to ensure access rights support the segregation of incompatible functions.
- Review of user accounts – system/ default/ generic
- Review of records for periodic review of existing users in the system
- Review of file system permissions
- Management of privileged access rights
- Management of secret authentication information of users
- Use of secret authentication information
- Other controls as applicable

#### 4.2.5.11 System acquisition, development and maintenance

Review should comprise of the following:

- Information security requirements analysis and specification
  - Securing application services on public networks
  - Protecting application services transactions
  - Secure development policy
  - System change control procedures
  - Technical review of applications after operating platform changes
  - Restrictions on changes to software packages
  - Secure system engineering principles
  - Secure development environment
  - Outsourced development
  - System security testing
  - System acceptance testing
  - Protection of test data
-

- Separation of development, testing and operational environments
- Installation of software on operational systems
- Management of technical vulnerabilities
- Restriction on software installation
- Other controls as applicable

#### 4.2.5.12 Digital Signature and Cryptography

Review process should comprise of the following:

- Policy on the use of cryptographic controls
- Key management
- Acquisition process of Digital Signature
- Usage and management of Digital Signature
- Other controls as applicable

#### 4.2.5.13 Backup management

Review of backup management process should be conducted as per the sampling methodology and should comprise of the following:

- Policies and procedures for backup management
- Review access control, physical security and integrity of backup data and its storage
- Review of backup restoration procedure checks
- Adherence to the policies and procedures
- Other controls as applicable

#### 4.2.5.14 Logging and monitoring

Review should comprise of the following:

- Review of log policy
- Review of Event logging
- Protection of log information
- Administrator and operator logs
- Clock synchronization

#### 4.2.5.15 Training and awareness programs for Information Security

Review of training and awareness program to ensure effective user of IT systems should comprise of the following:

- Review of induction/trainings programs conducted
- Review of process defined for conducting training sessions

- Review of awareness through sphere phishing attack

#### 4.2.5.16 Physical and Environmental Security management

The physical and environmental security management review should consist of the following activities:

- Physical security perimeter
- Physical entry controls
- Securing offices, rooms and facilities
- Protecting against external and environmental threats
- Working in secure areas
- Delivery and loading areas
- Equipment sitting and protection
- Supporting utilities
- Cabling security
- Equipment maintenance
- Removal of assets
- Security of equipment and assets off-premises
- Secure disposal or re-use of equipment
- Unattended user equipment
- Assessment of vulnerability towards natural calamities
- Assessment of any systems and delivery channels not available to end users due to external factors
- Fire protection systems, their adequacy and state of readiness
- General failure of systems as a whole due to external factors, and the related threat perception
- Working environment vis-à-vis adequacy of air conditioning and other infrastructure related setup
- Physical security and access control to server room/data centres areas where n/w devices reside
- Premises management
- Access card management
- Other security systems, their adequacy and monitoring
- Temperature and humidity level monitoring and controls
- Adherence to provisions of MCGM's Security Policy

- Other controls as applicable

#### 4.2.5.17 Human Resource Security Management

The review should consist of the following activities:

- Policies and procedures
- Screening of employees
- Terms and conditions of employment
- Management responsibilities
- Information security awareness, education and training
- Disciplinary process
- Termination or change of employment responsibilities
- Information Security Review
- Compliance with security policies and standards

#### 4.2.5.18 Business Continuity Management and Disaster Recovery

- Technical compliance review
- Compliance with legal and contractual requirements which includes Identification of applicable legislation and contractual requirements, Intellectual property rights, Protection of records, Privacy and protection of personally identifiable information, Regulation of cryptographic controls and other aspects if applicable
- Other controls as applicable

The review should consist of the following activities:

- Planning information security continuity
- Availability of BCP and DR
- Review of BCP and DR plan
- Implementing information security continuity
- Verify, review and evaluate information security continuity
- Availability of information processing facilities
- Verify, review and evaluate the BCP and DR drill reports.
- Other controls as applicable

#### 4.2.5.19 Hardware/ Software Configuration

- Verify the design and design effectiveness of installation/ testing and management standards for IT Hardware and Software components

#### 4.2.5.20 Operating Systems & Database system Review

The security controls review for Operating System & Database system should comprise of the following:

- Access Management
- User and group privileges
- System and user policies
- Remote access policies
- Logging mechanism
- Domain architecture and trust relationships
- Share permissions and definitions
- Service packs and hot fixes
- System services and applications
- Policies and procedures that govern its use
- Patch and Antivirus update
- Registry settings, including registry security permissions
- Profiles and log-in scripts

Understand the legal and statutory requirements related to using the applications in scope.

The bidder should also review other related procedures namely backup management, disaster recovery management, incident management, change management, and risk management processes for the applications in scope.

#### **4.2.6 SAP & Non-SAP Application Audit**

##### **4.2.6.1 SAP Technical Audit**

MCGM has implemented various modules of SAP across the organization. Following SAP Components have been implemented in MCGM:

- ✓ SAP SRM
- ✓ SAP CRM
- ✓ SAP MM
- ✓ SAP PS
- ✓ SAP HR
- ✓ SAP FICO
- ✓ SAP BI
- ✓ SAP RE
- ✓ SAP Fleet Management
- ✓ SAP Technical Control/ BASIS
- ✓ SAP EP
- ✓ SAP IS Utility

System Landscape details consisting of Development, Quality, Production environment is hosted at Primary Site (Ctrls DC) and Replication of Production Environment is hosted at Disaster Recovery site (Ctrls DR).

##### **4.2.6.1.1 SAP REVIEW**

Audit of the following minimum parameters needs to be carried out for SAP review, but not limited to:

1. Operational management
2. Risk management
3. Internal Audit
4. Organizational structure configured
5. Coding Standards as per SAP
6. Financial postings as per accounting standards
7. Encryption Review
  - a. Encryption of data volumes
  - b. Default key for data encryption
  - c. The SSL encryption to protect HTTP connection
  - d. The SNC encryption to protect the SAP GUI client connection
  - e. The SNC encryption to protect RFC connections between systems
  - f. The SSL encryption to protect SQL connections
8. Review of SAP instance i.e. SAP dialog, central, ICM, gateways parameters.
9. Review of table logging of critical tables
10. Identification and review of critical transactions and authorization objects.
11. Review of security guides, notes and security parameters
12. Review of trusted systems with low security levels
13. Reviews of various logs in the systems
  - a. Logging of security events
  - b. Logging of HTTP request



- c. Logging of table changes
- d. Logging of SAP gateway activities
- e. Logging of SAP assign privileges
- f. Logging of SAP System user activities
- 14. The auditor should also review followings:
  - a. Evaluating the SAP web dispatcher and SAP router against external vulnerabilities
  - b. Detouring payments
  - c. Espionage
  - d. Sabotage
  - e. Fraud
  - f. Date alteration
  - g. Developer trace
  - h. System trace
  - i. Inadvertent spoliation
  - j. Deliberate software spoliation

#### **4.2.6.1.2 SAP CONFIGURATION REVIEW**

Following minimum parameters needs to be carried out during the SAP configuration review, but not limited to:

- 1. Configuration review of devices hosting SAP such as database, servers, network devices, firewalls etc.
- 2. Various Security aspects of database w.r.t. to respective SAP Components and Best Practice in SAP environment
- 3. Review accessibility of various SAP system by end users, from within MCGM network and outside MCGM network
- 4. Review of system configuration
  - a. System monitoring document
  - b. SAP kernel updation
- 5. Review of data replication between primary and DR site
- 6. Review of DR switchover procedures
- 7. Review of change control process at ABAP instances
- 8. Review of change and transport management
  - a. Change management for moving the changes to production from development environment.
- 9. Review on SAP client
- 10. Review of patch management
  - a. Component updates
  - b. Kernel updates
  - c. SAP database updates
- 11. Review of background processing
- 12. Review of policies in accordance with business process requirement
  - a. SAP kernel upgrade policy
  - b. Database patch and version upgrade
  - c. OS patch and version upgrade
  - d. SAP change management

13. Software component and support pack level
  - a. Installed in development, quality, and production system
14. SAP services
  - a. Enterprise support report
  - b. EWA report
  - c. SOS report (Solution manager)

#### **4.2.6.1.3 SAP SYSTEM PENETRATION TESTING**

The bidder shall perform penetration testing for SAP, which is detailed, but not limited to, as mentioned below:

- a. SAP Application Penetration Testing
- b. Penetration testing of various production Instances within MCGM network.
- c. Internal and external network penetration testing of servers hosting SAP.
- d. Network security architecture review of network infrastructure supporting SAP.

#### **4.2.6.2 Application Security Testing (Applicable for SAP & Non-SAP Applications)**

Review the architecture of custom-developed web applications covering web server, database server and integration with external parties considering security aspects. The testing should be done on the applications (customer facing and internal) used within MCGM. A typical test case in this activity will be to check whether a user can bypass the login and get access into the application without password or unethically. This would include but not limited to analysis of following:

- Access rights, access privileges
- Application audit (input, output and processing)
- Application architecture
- Adherence to regulatory compliances
- Logical security review
- Audit trail and logging

The assessment should cover both business logic and technical risks. The assessment report should contain a detailed threat list of all the application. The threat list should contain the possible risks to the applications both from a business and technical aspect.

The bidder should attempt to identify and exploit vulnerabilities that include the OWASP top application security risks. The security audit should follow OWASP guidelines covering the followings, but not limited to:

- a. Injection
- b. Cross-Site Scripting (XSS)
- c. Broken Authentication and Session Management
- d. Insecure Direct Object References
- e. Cross-Site Request Forgery (CSRF)
- f. Security Misconfiguration
- g. Insecure Cryptographic Storage
- h. Failure to Restrict URL Access

- i. Insufficient Transport Layer Protection
- j. Invalidated Redirects and Forwards
- k. Input Validation flaws
- l. Malicious file execution
- m. Information leakage and improper error handling
- n. Insecure cryptographic storage
- o. Insecure communications
- p. Denial of Service

#### 4.2.6.2.1 APPLICATION CONTROL TESTING

Application control is a security practice that blocks or restricts unauthorized applications from executing in ways that puts data at risk. The control functions vary based on the business purpose of the specific application, but the main objective is to help ensure the privacy and security of data used by and transmitted between applications.

The objectives of application controls, which may be manual or automated, is to ensure the completeness and accuracy of the records and the validity of the entries made therein.

The application control testing should follow the guidelines covering the following, but not limited to:

- a. Application architecture
- b. Review application code for performance optimization
- c. Study for adequacy of input processing and output controls and conduct various tests to verify existence and effectiveness of controls.
- d. Logical access control, user maintenance and password
- e. Authorization mechanism and control (maker checker, exceptions etc)
- f. Review effectiveness and efficiency of the applications
- g. Complete review of application parameterization. Backup/fallback/restoration procedures and contingency planning.
- h. Review of segregation of roles and responsibilities with respect to application software to improve internal controls
- i. Review of customizations done to the software and the SDLC policy followed for such customization. Proposed change management procedure during conversion, migration of data, version control etc.
- j. Audit of application interfaces with other systems or interface of other system with application.
- k. Performance/ load testing of all public facing applications/ websites should be conducted. The vendor shall conduct following performance tests and provide reports in terms of speed, stability and scalability:
  - 1. Load test: verify the applications ability to work correctly with certain number of concurrent users
  - 2. Stress test: test an application under extreme workloads to see how it handles high traffic or data processing
  - 3. Volume test: populate large amount of data in database and monitor the overall software system's behavior
  - 4. Soak/ endurance test: test a system with a significant load extended over a significant period of time, to discover how the system behaves under sustained use

5. Phishing test: to analyze security features built in system
6. Ethical hacking: to analyze whether system is cloneable to hackers on website and networks

#### *4.2.6.2.2 SOURCE CODE REVIEW*

Secure Code Review is a process which identifies the insecure piece of code which may cause a potential vulnerability in a later stage of the software development process, ultimately leading to an insecure application. Source code review should be done for custom developed Non-SAP applications and custom development in SAP. The Source code review should follow the guidelines covering but not limited to the below:

- Automated source code vulnerability scan and analysis
- Manual source code review and assessment
- Coverage of source code vulnerabilities identification includes:
  - Usage of dangerous functions
  - Bad coding practices
  - Leftover debug codes
  - Unverified input data
  - System information leakage
  - Poor error handling
  - Command/sql injection
  - Cross site scripting
  - Weak password management
  - Poor generation of random numbers, etc.

#### *4.2.6.2.3 API SECURITY TESTING*

This testing is focused on the interfaces of the applications (customer facing and internal) where it interacts with another application for business purpose. Here, the authentication, integrity and confidentiality of API's request and response is tested using hacking tools. MCGM's internal and customer facing applications have multiple integration with SAP system & payment gateway as well.

#### *4.2.6.2.4 INTEGRATION TESTING/ REVIEW*

The integration testing would ensure that data flow between applications integrated with SAP or non- SAP and between applications and payment gateway is seamless and ensure confidentiality, integrity and availability.

#### *4.2.6.2.5 SYSTEM SECURITY REVIEW*

The Application security review of hosted application should be performed using tools with minimum manual intervention. During the grey box testing, it is expected to test the functionality of the application using more than one role and identify issues that cannot be found using automated scanners. Number of roles will be shared during the testing phase. Application Security testing shall include testing for common vulnerabilities mentioned in forums such as OWASP, but not limited to that should be performed are as listed. Selected bidder will carry out following grey box, black box, penetration tests, code review, and vulnerability assessment tests as per the request received from MCGM.

Tests to be conducted during **Grey Box** testing are following, but not limited to:

- a. Injection flaws such as SQL, OS etc.
- b. Cross site scripting test
- c. Broken access control test
- d. Session management & cookie management test
- e. Buffer overflow, invalid inputs, insecure storage etc.
- f. Improper error handling test
- g. Denial of service attack test
- h. Brute force attacks
- i. Insecure configuration management test inclusive of all layers i.e. Network,
- j. Operating system, database and application
- k. Password strength on authentication pages
- l. Exploitable hacking vulnerabilities
- m. Any other attacks, which can make MCGM's website and web-applications vulnerable

Tests to be conducted during **Black Box** testing are following, but not limited to:

- a. Check name server responses
- b. Examine network perimeter
- c. Conclude on architecture of the remote infrastructure
- d. Normal port scanning
- e. Port scanning with ids evasion techniques
- f. System fingerprinting (OS, Services, etc.)
- g. Improper error handling test
- h. Tool based vulnerability scan
- i. Password cracking, brute force attack
- j. Validation of the vulnerability and filtering of false positive.
- k. Exploitation of identified vulnerabilities
- l. Gain privileged account from successful exploits
- m. Scenario build up for denial of service attacks
- n. Other controls as applicable

Tests to be conducted during **Source Code** review are following, but not limited to:

- a. Format string missing
- b. Buffer overflow
- c. Memory leaks
- d. Security concerns on API's used
- e. Tests of black-box testing
- f. Other controls as applicable

Tests to be conducted during **Data Centre Server Security** review are following, but not limited to:

- a. Review of security parameters at SAP, database, operating system and hardware level
- b. Configuration review of servers
- c. Secure code review for DC applications
- d. Security review of complete DC infrastructure
- e. Review for any integrated services and components
- f. Security review as per OWASP top 10

Besides the following **Controls Review** also required to be conducted following, but not limited to:

- a. Operating systems server controls
- b. Database server controls
- c. Network security review as part of application security
- d. Integration with SAP application
- e. Fitment of application with dc infrastructure
- f. Enforcement of policies
- g. Segregation of duties
- h. Rights and privileges granted to users and authorization matrix
- i. Review of technical controls for SAP applications. Viz. Password controls, user administration, privileged users, auditing, change controls, batch job management, direct access to data through tables
- j. Review of IT policies and procedures related to SAP administration and maintenance and IT governance controls review (for SAP applications)

#### ***4.2.6.2.6 IDENTITY AND ACCESS REVIEW (APPLICABLE FOR SAP, NON-SAP APPLICATIONS AND MOBILE APPLICATIONS)***

Following minimum parameters needs to be carried out during the review of user management, but not limited to,

1. Review of role and authorization
  - a. Policies and procedures for account management, end user security policy and user access management
  - b. Review of list of users and corresponding user access request form as per the sampling methodology
  - c. Review of user access to ensure access rights support the segregation of incompatible functions.
  - d. Review of user accounts – system/ default/ generic
  - e. Review of records for periodic review of existing users in the system
  - f. Review of file system permissions
  - g. Management of privileged access rights
  - h. Management of secret authentication information of users
  - i. Use of secret authentication information
  - j. Other controls as applicable
2. Review of password policy at SAP and database level
  - a. Minimal password length
  - b. Number of invalid logons attempts before user account lock out
  - c. Minimal validity period of password
  - d. Password compliance with the security policies in place
3. Review and recommendations on default password for access to the application

4. Review of audit trail at SAP and database level
5. Review of SAP and database user management
  - a. Accounts with SAP\_ALL profile
  - b. Accounts with rights to start any program
  - c. Accounts with rights to modify critical tables
  - d. Accounts with rights to execute OS commands
  - e. Accounts with rights to assign privileges
  - f. Accounts with role content admin
  - g. RFC connections that store user authentication
6. Review of groups in SAP user profiles
7. Review of user creation, modification, deletion and deactivation process
8. Review of super user and administration user ids

#### **4.2.6.2.7 SYSTEM AND APPLICATION ACCESS MANAGEMENT**

Following minimum parameters needs to be carried out during the review of system and application access management, but not limited to:

1. Access control policy
2. Access to networks and network services
3. Information access restriction
4. Secure log-on procedures
5. Workflows for application access management
6. Password management system
7. Use of privileged utility programs
8. Review of Basis Administration
9. Review of SPOOL Administration
10. Access control to program source code
11. OS command access
12. Review of access to RFC
  - a. RFC function and queues
  - b. Control settings for RFC service (reginfo.dat)
  - c. Control settings for RFC service (secinfo.dat)
13. Other controls as applicable
14. Review of unauthorized access to
  - d. SAP control service functions
  - e. SAP host control service function
  - f. Message service function
  - g. The internal SAP TREXNet services

#### **4.2.6.2.8 DIGITAL SIGNATURE (APPLICABLE FOR SAP AND NON-SAP APPLICATIONS)**

Review of digital signature should comprise of the following, but not limited to:

- a. Key management
- b. Acquisition process of digital signature
- c. Usage and management of digital signature
- d. Other controls as applicable

#### **4.2.6.2.9 REVIEW OF PAYMENT GATEWAYS**

Review of security parameters related to payment gateways used by applications:

- a. Security parameters used in integration with application
- b. Encryption techniques
- c. Access control & Authentication
- d. Regulatory compliance followed at the payment gateway service provider

#### **4.2.6.2.10 DATABASE AUDIT**

The database configuration audit should include the following, but not limited to:

- a. Database account authentication
- b. Password policy
- c. Database account privileges
- d. Database auditing
- e. Database logging and tracing
- f. Database network access mechanism
- g. Database files and directories permission
- h. Access control and authentication
- i. Unnecessary services
- j. Remote login settings
- k. Patches and updates

#### **4.2.7 IT Audit for locations**

- Understand and review the Asset Management procedures- Including, but not limited to, local asset management policy/ procedures/ guidelines, ownership for asset management, maintenance of asset register, periodic review/validation of assets, etc
- Understand and review the Security Policy and/ or Procedures for OS Patch Management, Anti-virus & other security components deployment/ update, Change Management and Incident Management. Bidder shall also do testing on randomly selected systems to assess the implementation of defined policies.
- Security assessment of networks and network devices.
- Security configuration review of randomly selected desktops/ laptops/ thin clients to assess the overall security of the systems in order to prevent data leakage and protect against cyber threats.
- Following are the locations that needs to be audited from the above-mentioned scope.
  - MCGM, Head Office, CSMT
  - MCGM Ward office Pant Nagar, Ghatkopar
  - Any one ward offices of MCGM



#### 4.2.7.1 Endpoints review

Following are the review of the endpoints systems available at various locations of MCGM:

- Review of endpoint secure hardening guidelines
- Security controls and tools implemented on the endpoints
- User access review
- Administrative access control rights
- Password Policy
- Active directory policy

#### 4.2.7.2 End User Devices Security Scanning

The audit of end user devices such as desktops, laptops, tablets, etc should include the following, but not limited to:

- a. Vulnerability scanning of end user devices
- b. Security configuration review of all the end user devices
- c. Observe, analyse and assess the operations being performed from end user devices
- d. Analyse the vulnerability scanning report
- e. Detailed report on findings with suggestions and recommendations.
- f. Antivirus / OS patches / Latest OS

#### 4.2.7.3 Anti-virus and Patch management process

Review of anti-virus and patch management should comprise of the following:

- Policy and procedure for Virus management and patch management
- Review of Antivirus (AV) and patch management process as per the sampling methodology defined
- Schedule of AV updates and patch updates
- Security controls of AV server and patch update servers
- AV updates status reports, auditing and logging
- Review of AV log review records
- Review of controls against malware
- Other controls as applicable

#### 4.2.7.4 Desktop Review

Review of desktops (both connected to network and standalone should comprise of the following:

- Policy and procedure for desktop management

- Review of desktop controls
- Review of configuration for all workstations
- Review of desktop use policy
- Clear desk and clear screen policy
- Other controls as applicable

### **4.3 Compliance Review**

#### **4.3.1 Post Implementation (Compliance) Review:**

The objective of this activity is to conduct revalidation of the issues found during the audit and assess compliance w.r.to recommended remedial steps.

#### **Confirmatory Review:**

The objective of this activity is to conduct second level confirmatory review once the compliance review is completed to ensure that the gaps identified in the compliance review is fulfilled.

### **4.4 Other Components and Reporting**

A draft report should be prepared for each type of audit, each type of applications and each type of office in case of IT Infrastructure. The report should also include all the controls/ test cases that were reviewed during audit.

The report should cover executive summary, activities covered; scope coverage and detailed observations for each area and should be in the format as mentioned in Annexure IX– section of the report. Each observation should have a risk rating, impact assessment, relevant ACT/ Guidelines/ Policy/ Standard, detailed steps with screenshots for remediation and con. Audit supporting should be provided in the report in the form of tables, screen shots, images etc.

Based on the analysis, the report should provide a detailed set of recommendations with milestones on how to mitigate the identified security risks, including recommendations. The recommendations should be direct and concise and not anecdotal. They should provide mitigation plans with documentation to assist the organization in the growth and support plans of the systemization. In addition, the recommendations should measure the alignment of the assessed systems with reference to proven industry best practices.

In addition to final report, a signed security compliance certificate should be submitted to MCGM for the applications in the format mentioned in Annexure IX– section of the report.

The key activities shall comprise of the following:

- Prepare a draft report highlighting the gaps observed basis the final review

- Discuss the draft report and audit findings with the management
- Obtain management comments
- Present the report to the management
- Prepare and submit Security Compliance Certificate/Report
- Acceptance of the final report/certificate and the risk acceptance of the open items from the audit.
- Release the final report

Planning, compliance review and reporting activities to be included for compliance review of open observations from previous IT Audit.

#### 4.4.1 Description of applications and details on in-scope IT infrastructure components

Following tentative applications shall be included in the scope for the Systems Audit activity.

Sr. No	Name of the application	Description of application
<b>SAP Applications</b>		
1.	SAP SRM	Supplier Relationship Management
2.	SAP CRM	Customer Relationship Management which includes 84 services
3.	SAP MM	Material management
4.	SAP PS	Project Management
5.	SAP HR	The module manages processes such as Organization Management, Personnel Administration, Recruitment, Leave Management, Appraisal Management, Training and Event Management and MIS.
6.	SAP FICO	Finance and control
7.	SAP BI	The application acts as a reporting tool for information on customers, vendors, financials, etc.
8.	SAP RE	The application automates rental management for properties under MCGM by managing processes such as tracking rental agreement, issuing challan/ receipt to tenants, tracking receivables
9.	SAP Fleet Management	Caters to a vast and varied fleet of Solid Waste Management, Hospitals, Fire Brigade, Engineering and office vehicles, Allocation of Vehicles from almost 100 garages spread across the city against various indents, maintaining history of vehicles trip, vehicle-wise cost and maintenance.
10.	SAP Technical Control/ BASIS	"Password controls, user administration, privileged users, auditing, change controls, batch job management, direct access to data through tables"
11.	SAP EP	SAP Enterprise Portal
12.	SAP IS Utility	The module for all kind of utilities such as water supply etc.

<b>Sr. No</b>	<b>Name of the application</b>	<b>Description of application</b>
<b>Non-SAP Applications</b>		
<b>13.</b>	CVS	<p>"Capital Value System application enables MCGM to assess and collect property tax. Key business processes automated by this application are:</p> <ol style="list-style-type: none"> <li>1.Assessment</li> <li>2.Bill/ Demand generation</li> <li>3.Printing and Distribution</li> <li>4.Collection of Tax Revenues</li> <li>5.MIS Reporting</li> </ol>
<b>14.</b>	AQUA	<p>"The 'Water Bill Collection' or 'AQUA Super' application makes the water billing and collection process simpler for residents having an MCGM water connection; additionally, it also benefits the department by streamlining the process of bill generation and tracking receivables. Key business processes automated by this application are:</p> <ol style="list-style-type: none"> <li>1.Meter Reading Entry</li> <li>2.Billing / Demand Generation</li> <li>3.Printing and Distribution</li> <li>4.Collection of Water Bills</li> <li>5.MIS Generations</li> </ol>
<b>15.</b>	GIS DP	<p>The suite of GIS application was developed to cater to the needs of property tax department, sewerage department and estate department.</p> <p>The key features offered by the application for Development and Planning (DP) department include:</p> <ul style="list-style-type: none"> <li>• User Administration Module</li> <li>• User Authentication Module</li> <li>• Map Browsing Module</li> <li>• Database update module</li> </ul>

<b>Sr. No</b>	<b>Name of the application</b>	<b>Description of application</b>
		<ul style="list-style-type: none"> <li>• Database Search Module</li> <li>• Generate Reports Module</li> <li>• Tools Module</li> </ul>
<b>16.</b>	GIS SO	<p>The suite of GIS application was developed to cater to the needs of property tax department, sewerage department and estate department.</p> <p>The key features offered by the application for sewerage department include:</p> <ul style="list-style-type: none"> <li>• Reports based on geographical area providing details of manholes, bypass lines, ventilation columns and pumping mains. The non-spatial reports provide information on line diameter, line status, line capacity, slippages in maintenance and manhole/ vent shaft repair history.</li> <li>• The application also allows user to create, modify (merge, split etc.) and delete sewer lines on the GIS maps as per the changes made on field to maintain an updated record of the changes occurring on a day to day basis.</li> </ul>
<b>17.</b>	AutoDCR	Application for online building proposal
<b>18.</b>	eOffice	Application for managing official files
<b>19.</b>	GIS	GIS applications and its integration with other applications
<b>20.</b>	GIS A&C	GIS application that is aimed at supporting property tax collection process.
<b>21.</b>	Rain Gauge	This web application is used to display specific MCGM info, here we display Weather Forecast, Weather warning, Traffic diversion, Monsoon Report, Ward directory and Ward maps info in pdf format. It also display Live Update of rain fall for different location in Mumbai and details about Temperature, Humidity, Wind, Pressure and Rain Fall data and Today's Tide data. we also get Temperature, Humidity, Wind, Pressure and Rain Fall data from google map in popup from this page.

<b>Sr. No</b>	<b>Name of the application</b>	<b>Description of application</b>
<b>22.</b>	Command & Control	Command and Control system is designed to log and process disasters with the help of maps, it's objective is to provide ease in process of reporting disasters, processing with actions, real time messaging to concerned officers, summarizing whole process with the reports.
<b>23.</b>	VTMS	Vehicle Tracking Management System
<b>24.</b>	DMS	Document Management System
<b>25.</b>	LMS	Legal Management System of SAP
<b>26.</b>	HMIS	Health Management and Information Systems
<b>27.</b>	Android based mobile applications	My License, My Property Tax, My Complaints, Water Bill Payment, Shops & Establishments, Birth & Death Info etc.
<b>28.</b>	IOS based mobile applications	My License, My Property Tax, My Complaints, Water Bill Payment, Shops & Establishments, Birth & Death Info etc.

#### 4.4.2 Details of the existing IT landscape and Infrastructure of MCGM:

##### Non-IT components at WDC:

Sr. no.	Description	Qty
1	Firefighting system (fire alarm suppression system with 250 smoke detector)	2
2	Fire alarm system	1
3	Fire suppression system FM200 cylinder old DC 4 nos with smoke detector	1
4	Fire suppression system FM200 cylinder new DC 8 nos with smoke detector	1
5	Fire suppression system FM200 EPBX room room 2 nos with smoke detector	1
6	Fire suppression system FM200 meter room 3 nos with smoke detector	1
7	Fire suppression system FM200 UPS Room 1 nos with smoke detector	1
8	Access Control Panel (spectra act 1000)	2
9	Access Control Panel (spectra act 500)	2
10	EPABX System	1
11	DG Set 250 Kva kirloskar	1
12	DG Set 100 Kva cumin	2
13	DG set 125 ws-b kirloskar	1
14	DG Set 500 Kva	2
15	70 KVA + 1 redundant module (2 MHO 2-Worli data center)	4
16	UPS New DC 100 KVA (2*400 KVA)	8
17	Rack Power Distribution Units	25
18	Fire extinguishers Cylinder	30
19	Electrical Rooms	5
	<b>Total Tentative Non-IT Components (WDC)</b>	<b>91 Nos.</b>



**Network Devices available at Worli Datacenter:**

<b>Sr.No</b>	<b>Device Name</b>	<b>Device Count</b>
1	Router –Cisco 7206 with STM card	8
2	Switch –Cisco 2960S	9
3	Switch - Cisco 3750G – 12S	9
4	Switch - Cisco 3560X – 24T- S	1
5	Switch –Cisco 3560X	1
6	Switch –HP 5120 24G	5
7	Network MPLS links between Ward locations and WDC	2
8	Internet Link	2
9	P2P link between Ctrl's Cloud and WDC	1
	<b>Total Tentative Network Components (WDC)</b>	<b>38 Nos.</b>

**Security devices at WDC:**

<b>Sr.No</b>	<b>Device Name</b>	<b>Device Count</b>
1	Firewall	2
2	Firewall Analyzer	1
3	Cisco AMP Endpoint protection solution (Centralized system for multiple endpoints)	2
4	Proxy solution	1
5	NAC (Network Access Control)	2
	<b>Total Tentative Security Components (WDC)</b>	<b>8</b>

**Other Hardware hosted at Worli Datacenter:**

S.No.	Product	Description	Qty
1	Dell Blade Chassis	PowerEdge M1000E	2
2	Dell Blade Server	PowerEdge M910	8
3	Dell Enclosure Controller	PowerVault MD3600f	2
4	Dell Disk Storage Enclosure	PowerVault MD1200	18
5	Symantec Appliance	Symantec Netbackup 5230	2
6	Symacntec Disk Storage	Symacntec Disk Storage	3
7	Wipro Server	Net Power	2
	<b>Total Tentative Server Hardware + Backup Infra + Storage (WDC)</b>		<b>37 Nos.</b>

**Production Servers/VM at Worli Datacenter:**

S.No.	Server/VM	Operating System	Qty
1	Production Server/VM	Microsoft Windows Server 2008 R2 (64-bit)	12
2	Production Server/VM	Microsoft Windows Server 2003 (32-bit)	1
3	Production Server/VM	Microsoft Windows Server 2012 (64-bit)	6
4	Production Server/VM	CentOS 4/5/6/7 (64-bit)	4
5	Production Server/VM	Red Hat Enterprise Linux 6 (64-bit)	7
6	Production Server/VM	Red Hat Enterprise Linux 7 (64-bit)	4
7	Production Server/VM	Ubuntu 20.04LTS	1
8	Production Server/VM	Other Operating systems	7
	<b>Total Tentative Server/VMs (WDC)</b>		<b>42 Nos.</b>

**Other Components**

S.No.	Components	Qty
1	Public IP	35 Nos.
2	Endpoints (Desktops/Laptops)	50 Nos.

**Cloud Infrastructure:****SAP Servers hosted at Cloud/datacenter:**

S.No.	Server/VM	Operating System	Qty
1	SAP Server/VM	Microsoft Windows Server 2008 R2 (64-bit)	2
2	SAP Server/VM	Microsoft Windows Server 2012 (64-bit)	4
3	SAP Server/VM	Red Hat Enterprise Linux 5 (64-bit)	45
4	SAP Server/VM	Red Hat Enterprise Linux 6 (64-bit)	73
5	SAP Server/VM	Red Hat Enterprise Linux 7 (64-bit)	1
	<b>Total Tentative SAP VM Systems (Cloud)</b>		<b>125 Nos.</b>

**Non-SAP Systems hosted at Cloud/datacenter:**

S.No.	Server/VM	Operating System	Qty
1	Non-SAP Server/VM	CentOS 4/5/6/7 (64-bit)	1
2	Non-SAP Server/VM	Microsoft Windows Server 2008 R2 (64-bit)	12
3	Non-SAP Server/VM	Microsoft Windows Server 2012 (64-bit)	23
4	Non-SAP Server/VM	Red Hat Enterprise Linux 4 (32-bit & 64-bit)	2
5	Non-SAP Server/VM	Red Hat Enterprise Linux 5 (64-bit)	6
6	Non-SAP Server/VM	Red Hat Enterprise Linux 6 (64-bit)	35
7	Non-SAP Server/VM	Red Hat Enterprise Linux 7 (64-bit)	11
8	Non-SAP Server/VM	Ubuntu Linux (64-bit)	1
	<b>Total Tentative Non-SAP VM Systems (Cloud)</b>		<b>91 Nos.</b>

**Physical Host Servers on Cloud:**

S.No.	Server/VM	Qty
1	Physical Host for SAP & Non-SAP Virtual machines (Dell R730 Servers with 44 Physical Cores, 1 TB RAM)	12
2	Dedicated servers (Dell Servers)	06
	<b>Total Tentative Physical servers (Cloud)</b>	<b>18 Nos.</b>

**Other Components on Cloud:**

S.No.	Components	Qty
1	Public IP	175 Nos.
2	Backup Infrastructure	193 Nos.

**Network Components on cloud:**

Sr.No.	Device Name	Quantity
1.	Internet Links at Ctrl's cloud	2
2.	MPLS links between WDC and Ctrl's cloud	2
3.	Network Switches	2
4.	Router	2
<b>Total Network Components (Cloud)</b>		<b>8 Nos.</b>

**Security Components on Cloud:**

Sr.No.	Device Name	Quantity
1.	Fortigate Firewalls	2
2.	SSL Certificate	75
3.	VPN Users	67
4.	DNS	2
<b>Total Security Components at Ctrl's cloud</b>		<b>146 Nos.</b>

**Process Review:**

<b>S. N</b>	<b>Scope of Work</b>	<b>Qty.</b>
<b>1</b>	Audit overall IT operations as per ISO 27001 framework	<b>1</b>
<b>2</b>	Authorization and Segregation of Duties Controls	<b>1</b>
<b>3</b>	Assessment of Role based security under scope	<b>1</b>
<b>4</b>	Organizational Policies and Procedure	<b>1</b>
<b>5</b>	Change Management	<b>1</b>
<b>6</b>	Incident Management	<b>1</b>
<b>7</b>	Asset Management	<b>1</b>
<b>8</b>	Third Party Management	<b>1</b>
<b>9</b>	System and Application Access Management	<b>1</b>
<b>10</b>	User Access Management	<b>1</b>
<b>11</b>	System acquisition, development and maintenance	<b>1</b>
<b>12</b>	Digital Signature and Cryptography	<b>1</b>
<b>13</b>	Backup Management	<b>1</b>
<b>14</b>	Logging and Monitoring	<b>1</b>
<b>15</b>	Training and awareness programs	<b>1</b>
<b>16</b>	Physical and Environmental Security	<b>1</b>
<b>17</b>	Human Resource Security	<b>1</b>
<b>18</b>	Business Continuity Management	<b>1</b>
<b>19</b>	Hardware/Software Configuration	<b>1</b>
<b>20</b>	Operating System & Database Review	<b>1</b>
	<b>Total</b>	<b>20</b>

#### 4.4.3 Standards to be followed during review/ audit

The standards recommended to be followed for deciding the scope of work are as follows:

<b>Audit Scope</b>	<b>Standards/ Documents to be followed</b>
SAP Security Audit	<ul style="list-style-type: none"> <li>○ Security Guidelines by SAP / EWA</li> <li>○ Business Blueprint and other documents</li> <li>○ CVC Guidelines</li> <li>○ IT Act 2000</li> </ul>
Vulnerability Assessment and Penetration Testing of Servers and Network Devices	<ul style="list-style-type: none"> <li>○ NIST 800-115</li> <li>○ ISO 17799</li> <li>○ ISO 27002</li> </ul>
Penetration Testing of applications	<ul style="list-style-type: none"> <li>○ OWASP (Open Web Application Security Project) Top 10</li> </ul>
Cloud Security	<ul style="list-style-type: none"> <li>○ CSA Framework</li> <li>○ ISO 17799</li> <li>○ ISO 27002</li> </ul>
Server and Operating System Security Review	<ul style="list-style-type: none"> <li>○ NIST 800-123 Guide to General Server Security</li> <li>○ CIS Benchmark</li> <li>○ ISO27001:2013</li> </ul>
IT Process Audit	<ul style="list-style-type: none"> <li>○ ISO 27001:2013</li> <li>○ IT Act 2000</li> <li>○ Maharashtra Public Record</li> <li>○ MCGM IT Policy &amp; Procedures</li> <li>○ MCGM Procurement Policy and other guidelines</li> <li>○ State eGovernance /IT Policy</li> <li>○ CVC Guidelines</li> <li>○ MCGM Act</li> <li>○ ISO 17799</li> </ul>
Business Continuity and Disaster Recovery	<ul style="list-style-type: none"> <li>○ ISO22301</li> </ul>
Network devices and Firewall review	<ul style="list-style-type: none"> <li>○ <a href="#">ISO/IEC 27033</a></li> <li>○ CIS Benchmark</li> <li>○ ISO27001:2013</li> <li>○ ISO 17799</li> <li>○ ISO 27002</li> </ul>
Database Review	<ul style="list-style-type: none"> <li>○ CIS Benchmark</li> </ul>
Email Security	<ul style="list-style-type: none"> <li>○ Cert-In Guidelines CIGU-2011-0153</li> <li>○ NIST 800-45</li> <li>○ ISO 17799</li> <li>○ ISO 27002</li> </ul>

However, the auditor would identify and audit as per all regulations applied to the organization.

#### **4.4.4 Deliverables**

The following set of deliverables needs to be submitted by the bidder for each round of audit:

- Review plan and schedule
- Progress Reports as decided by MCGM
- List of standards and regulations that MCGM required to follow to ensure confidentiality, integrity and availability of data.
- Review Report. The report should contain:
  - Identification of auditee
  - Date, time and location of the audit
  - Mapping of observation with the standard and specific control in the standards.
  - Comments against each control tested
  - Summary of audit findings including identification tests, tools used and results of tests performed (like vulnerability assessment, penetration testing, application security audit etc.)
  - Detailed review approach and methodology
  - Tools used and methodology employed
  - Positive security aspect identified
  - List of vulnerability identified
  - Description of vulnerability
  - Risk rating or severity of vulnerability
  - Category of risks: Very High/ High/ Medium/ Low
  - Test cases used for the assessing the vulnerabilities
  - Illustration of the test cases
  - Proof/evidence (Screenshot) of the vulnerabilities identified
  - Mapping of evidences with observations in the report.
  - Analysis of vulnerability and issue of concern
  - Recommendation with detailed implementation steps / screenshots for corrective action as per industry standard and best practices.
  - Dashboard for audit observations and compliance
- All the summary reports submitted should be signed by technically qualified persons and he/she should take ownership of document submitted to MCGM.
- Post Compliance Review report after implementing the recommendations.
- Final detailed review report Recommendations along with detailed solutions.

In addition to the list mentioned above, the report must also have the following sections:

- ❖ Executive Summary
- ❖ Scope of Work
- ❖ Audit activities performed
- ❖ Evidences
- ❖ Conclusion

**Note:**

- Successful audit agency shall submit the schedules and pre-requisites for audits 15 days prior to the activities.
- Workshop/ Session materials prepared by the audit agency for MCGM purpose will be MCGM's intellectual property.
- Vulnerability assessment and Penetration Testing should cover MCGM's Information Systems Infrastructures which includes Network Devices, Security Devices, Servers, Operating Systems, Databases, Applications, System configured with External IP's , websites, etc. in the locations provided by MCGM.



#### 4.4.5 Minimum Qualifications & Experience for key Resources

The following are minimum qualifications and experience for key resources required to implement Systems Audit and Security Audit of IT Infrastructure. The following personnel would be required during the project planning, review and reporting audit activities. The team composition for both the Audit programs, i.e. Systems Audit and Security Audit of IT Infrastructure should be conducted from MCGM premises. The number of resources

##### **Systems Security Review**

#	Role	Min. Qualification & Experience
1	Project Manager	<ul style="list-style-type: none"> <li>• B.E. / B.Tech./ BCA/ MCA + M.B.A.</li> <li>• 7+ Years of experience in Information Security</li> <li>• CISSP/CISA certified</li> </ul>
2	Senior Consultant	<ul style="list-style-type: none"> <li>• B.E. / B.Tech.</li> <li>• 4+ Years of Experience in Information Security</li> <li>• CISA/CISSP/ISO 27001 Lead Auditor (L.A.) certified</li> </ul>
3	Consultant	<ul style="list-style-type: none"> <li>• B.E. / B.Tech.</li> <li>• 2+ Years of Experience in Information Security</li> <li>• CISA/CISSP/ ISO 27001 Lead Auditor (L.A.) certified</li> </ul>

##### **IT Process Review**

#	Role	Min. Qualification & Experience
1	Project Manager	<ul style="list-style-type: none"> <li>• B.E. / B.Tech./ BCA/ MCA (mandatory) + M.B.A.</li> <li>• 7+ Years of experience in Information Security</li> <li>• CISSP/CISA qualified</li> </ul>
2	Senior Consultant	<ul style="list-style-type: none"> <li>• B.E. / B.Tech.</li> <li>• 4+ Years of Experience in Information Security</li> <li>• CISA/CISSP/ISO 27001 Lead Auditor (L.A.)</li> </ul>
3	Consultant	<ul style="list-style-type: none"> <li>• B.E. / B.Tech.</li> <li>• 2+ Years of Experience in Information Security</li> <li>• CISA/CISSP/ ISO 27001 Lead Auditor (L.A.) certified</li> </ul>

**Security Review of IT Infrastructure**

#	Role	Min. Qualification & Experience
1	Project Manager	<ul style="list-style-type: none"><li>• B.E. / B.Tech./ BCA/ MCA (mandatory) + M.B.A.</li><li>• 7+ Years of experience in Information Security</li><li>• CISSP/CISA qualified</li></ul>
2	Senior Consultant	<ul style="list-style-type: none"><li>• B.E. / B.Tech.</li><li>• 4+ Years of Experience in Information Security</li><li>• CISA/CISSP/ISO 27001/CEH/CCNA</li></ul>
3	Consultant	<ul style="list-style-type: none"><li>• B.E. / B.Tech.</li><li>• 2+ Years of Experience in Information Security</li><li>• CISA/CISSP/ISO 27001/CEH/CCNA</li></ul>

However, if it is discovered that the personnel deployed to carry out the specified work do not meet the minimum qualifications as stated above, the bidder shall have to replace the personnel of concern with personnel having minimum qualifications immediately. The CV of the deployed personnel to be shared before start of audit.

**4.4.6 Operational Procedure**

- The audit will be control checklist based where observations will be noted for all controls. The evidences should be mapped to audit observations.
- Compliance audit to be conducted after minimum compliance of 80%. However, MCGM management can decide the compliance percentage over and above.
- The audit report provided by the bidder should have details of corrective actions of steps to remove identified vulnerabilities. Auditor should provide the methodology sequence of steps to close the observation.
- Compliance audit should be done not only to check for removal of previously identified threats but also to ensure infrastructure and systems has no vulnerability as a result of closure of certain observations.
- Black Box testing for security audit should follow OWASP (Open Web Application Security Project) guidelines though not only limited to the same.
- The following audit environment should be used during audit

<b>Audit Scope</b>	<b>Audit Environment</b>
Application Security Audit	Production
Segregation of Duties	Production
Code Review	Production
Vulnerability Assessment and Penetration Testing of Servers and Network Devices	Production
Penetration Testing of applications	Production
Cloud Security	Production
Server and Operating System Security Review	Production
Network devices and Firewall review	Production
Database Review	Production
Email Security	Production
Endpoint Security	Production
Digital Forensics Readiness assessment	Production

- MCGM shall not provide any tools that may be required by the successful bidder for conducting the systems and infrastructure security audit.
- All the software, hardware equipment like Laptops, tools etc. to carry out the assignment has to be brought by the selected Bidder at no extra cost. Selected Bidder will use audit tools that are licensed and not the trial versions. Auditor should disclose the details of automated tools used for accomplishing the audit process. The auditor must have the valid license of the said automated tool(s). Details of the Audit tools to be used should be provided to MCGM.
- MCGM will not make any additional payment for usage of tools proposed by the successful bidder. Also MCGM will also not have any rights to those tools after the completion of work.
- Successful bidder is expected to clearly stipulate activities that will be conducted onsite (at Datacentre / Disaster Recovery Site) and those that will be carried out from the bidder's premises.

- Successful bidder shall share the qualification details of the auditor prior to every assessment at MCGM. The auditors selected post qualification screening should be allowed to conduct the audit.
- The tools used for scanning (VA-PT, application security, SOD, code review etc.) should be the tools mentioned in leader or challenger quadrant of the latest “Gartner Magic Quadrant for Application Security” report.

## 5 Service Level Agreements

The purpose of this Service Level Requirements/Agreement (hereinafter referred to as SLR/SLA) is to clearly define the levels of service which shall be provided by the Service Provider to the department for the duration of this contract period of the Project.

The services are required for a period of 1 year from the date of Letter of Intent (LOI) / Out Line Agreement (OLA). The services to commence within 15 days from the date of LOI/LOA.

Successful bidder should arrange resource for review within 15 days from the receipt of the request from MCGM. Upon approval of deployment of resources, the bidders agencies need to deploy the resources with required skills and experience within a period of 15 days from the intimation by the User/IT Department.

#	Area	Expected Output	Penalty
1	Team mobilization	Within 15 days of award of LOI / LOA	Rs. 3000 per day of delay
2	Adherence to planned schedule and submission of the respective deliverable.	To meet the scheduled deadline as agreed with MCGM and documented in the purchase order for specific work.	Rs. 5,000 for the first week and Rs. 10,000 for every subsequent week subject to a maximum of 10% of the value of the specific work, post which MCGM may invoke the bidder. The penalty will be levied for reasons that are solely attributable to the agency.

### 5.1 Maximum Penalty

The SLA shall commence from the day of award of contract.

Maximum Penalty will be limited to the cost of breakups in the reference tables, subject to overall implementation schedule is not delayed beyond timelines committed by the bidder.

The sum total of all the penalties can be upto 10% of the contract, post which MCGM may invoke annulment of contract.

### 5.2 Risk Purchase Clause

1. In the event Selected Agency fails to execute the project as stipulated in the Contract Agreement, or as per the directions given by MCGM from time to time, MCGM reserves

the right to procure similar services from the next eligible Bidder or from alternate sources at the risk and cost of the Selected Agency. Before taking such a decision, MCGM shall serve a notice period of one month to the Selected Agency.

2. The 30-day notice period shall be considered as the 'Cure Period' to facilitate the Selected Agency to cure the breach. The provision for Risk Purchase shall be evoked in the event the Selected Agency fails to correct the breach within the 'Cure Period'.
3. The Selected Agency's liability under the resultant Agreement shall be determined as per the Law in force for the time being. The Selected Agency shall be liable to MCGM for loss or damage occurred or caused or likely to occur on account of any act of omission on the part of the Selected Agency and its employees.

**6 Payment Terms and Schedule**

1. Payment will be linked to delivery of the Audit Report and Compliance Report.
2. When the work awarded is related to conducting audit, 100% of the payment shall be released based on approval of the Preliminary Report and support extended to the development agencies for removal of the vulnerabilities.
3. When the work awarded is related to conducting Compliance Audit, 100% of the payment shall be released based on approval of the Compliance Report
4. The contract would be valid for a period of one years from the date of release of LOI/contract.
5. The price quoted in the price bid should cover all charges as mentioned deliverable in the scope.
6. All prices quoted should in Indian Rupees (INR).
7. MCGM will release the payment after submission of valid invoice subject to the condition that invoice and all supporting documents produced are in order and work is performed to the satisfaction of User Department of MCGM.
8. Report shall not be considered as submitted without a written concurrence from MCGM.
9. MCGM shall be entitled to delay or withhold the payment of any invoice or part of it delivered by Agency, when MCGM disputes such invoice or part of it, provided that such dispute is bonafide.
10. It is mandatory for the contractors to open a Bank Account in any of the banks approved by MCGM (specified in Annexure of the document) for easy and quick payments. All payments under the contract will be made only on this Bank Account through Electronic Clearing System/ RTGS/ NEFT/ CBS.
11. Successful bidder need to submit Irrevocable Undertaking (Annexure) regarding GST.

## **7 Annexure I: Pre-Qualification Documents**

### **7.1 Pre-Qualification Cover Letter**

Date: dd/mm/yyyy

To

<Insert complete postal address>

**Sub : Implementation of IT Audit at Municipal Corporation of Greater Mumbai**

**Ref : Bid No:<No> Dated <DD/MM/YYYY>**

Dear Sir,

Having examined the bid, the receipt of which is hereby duly acknowledged, we, the undersigned, offer to provide the professional services as required and outlined in the bid for the **Selection of Service Provider for Implementation of IT Audit at Municipal Corporation of Greater Mumbai**.

We attach hereto our responses to pre-qualification requirements and technical and commercial bids as required by the bid. We confirm that the information contained in these responses or any part thereof, including the exhibits, and other documents and instruments delivered or to be delivered to Municipal Corporation of Greater Mumbai, are true, accurate, verifiable and complete. This response includes all information necessary to ensure that the statements therein do not in whole or in part mislead the Corporation in its short-listing process.

We fully understand and agree to comply that on verification, if any of the information provided here is found to be misleading the selection process, we are liable to be dismissed from the selection process or termination of the contract during the project, if selected to do so.

We agree for unconditional acceptance of all the terms and conditions set out in the bid document and also agree to abide by this bid response for the bid validity period as



mentioned in the RFP. We hereby declare that in case the contract is awarded to us, we shall submit the contract performance guarantee bond in the form prescribed in the bid.

We agree that you are not bound to accept any bid 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 bid 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.

---

Signature of Authorized Signatory (with official seal)

Name :

Designation :

Address :

Telephone :

E-mail address :

## 7.2 Format to Share Bidder's Particulars

#	Description	Details (to be filled by the responder to the Bid)
1.	Name of the company	
2.	Official address	
3.	Phone No. And Fax No.	
4.	Corporate Headquarters Address	
5.	Phone No.	
6.	Web Site Address	
7.	Details of Company's Registration (Please enclose copy of the company registration document)	
8.	Name of Registration Authority	
9.	Registration Number and Year of Registration	
10.	GST Registration No.	
11.	Permanent Account Number (PAN)	
12.	Company's Revenue for last 3 years (Year wise)	
13.	Company's net worth for the last year (FY 2020-21)	

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

Contact Details of officials for future correspondence regarding the bid process:

Details	Authorized Signatory	Secondary Contact
Name		
Title		
Company Address		

Phone		
Mobile		
E-mail		

**7.3 Format to Share Project Status**

<Company Letter Head>

Date: dd/mm/yyyy

To

<Insert complete postal address>

**Sub** : Certificate for <Project Name with Client Name>

**Ref** : Bid No:<No> Dated <DD/MM/YYYY>

Dear Sir,

I, \_\_\_\_\_, on behalf of M/s \_\_\_\_\_ certify that as per work order number \_\_\_\_\_ issued by MCGM for the project implementation of **Selection of Service Providers for Implementation of IT Audit at Municipal Corporation of Greater Mumbai** commenced work on <date>. The overall value of the contract with <Client Name> is INR <Project Outlay in INR> and the value for the application is INR\_\_\_\_\_

The engagement period of M/s\_\_\_\_\_ is from <Month and Year> to <Month and Year> and the application is currently under implementation/ UAT/operational/ defunct.

<Signatory

Name>

<Designation>

<Stamp>

**7.4 Format for Declaration by the Bidder for not being Blacklisted / Debarred**

(On Stamp Paper of Rs 500/- duly notarized)

**DECLARATION CUM-INDEMNITY BOND**

Date: dd/mm/yyyy

I, \_\_\_\_\_ of \_\_\_\_\_  
\_\_\_\_\_, do hereby declared and undertake as under.

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

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

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

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

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

6) I Indemnify Municipal Commissioner and the other officers of MCGM or their agents for any Damages, Loss, or Injury, any legal suit, proceeding or legal action whatsoever that may be caused at any time by me or any other staff of \_\_\_\_\_ company, for the work \_\_\_\_\_

undertaken and all such damage, damages, injury or loss, legal suit, legal action, I shall be solely responsible in individual as well as official capacity and such loss, damages, injury shall be made good and/ or as the case may be shall be paid immediately by me / Company to the satisfaction of the MCGM.

Dated \_\_\_\_\_ day of \_\_\_\_\_, 20\_\_\_\_

Identified by me

Before me

**7.5 Bank Guarantee**

(For a sum of 10% of the value of the contract)  
(With Stamp duty of 0.5 % on the total amount)

Ref. No. :

Date :

Bank Guarantee No. :

To

<Insert complete postal address>

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

inhabitants carrying on business at -----  
-----  
-----

in Mumbai under the style and name of Messers -----  
-----  
-----

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

THE MUNICIPAL COMMISSIONER FOR GREATER MUMBAI (hereinafter referred to as  
'the Commissioner' which expression shall be deemed, also to include his successor or  
successors for the time being in the said office of Municipal Commissioner) of the third part  
and THE MUNICIPAL CORPORATION OF GREATER MUMBAI (hereinafter referred to as  
'the Corporation') of the fourth part WHEREAS the contractors indemnify and keep  
indemnified the Corporation against any loss or damage that may be caused to or suffered by  
the Corporation by reason of any breach by the contractors of any of the terms and conditions

of the contract that will be entered subsequently (within 15 days) and/or in the performance thereof against Letter of Intent number ----- dated ----- for the project **Implementation of IT Audit at MCGM** of ----- department having tender No. <<>> tender amount Rs.----- and the terms of such tender / contract require that the contractors shall deposit with the Commissioner as earnest money and/ or the security a sum of Rs.----- (Rupees-----) AND WHEREAS if and when any such tender is accepted by the Commissioner, the contract to be entered into in furtherance thereof by the contractors will provide that such deposit shall remain with and will be appropriated by the Commissioner towards the Security Deposit to be taken under the contract and be redeemable by the contractors, if they shall duly and faithfully carry out the terms and provisions of such contract and shall duly satisfy all claims properly chargeable against them thereunder AND WHEREAS the contractors are constituents of the Bank and in order to facilitate the keeping of the accounts of the contractors, the Bank with the consent and concurrence of the contractors has requested the Commissioner to accept the undertaking of the Bank hereinafter contained, in place of the contractors depositing with the Commissioner the said sum as earnest money and/or the security as aforesaid AND WHEREAS accordingly the Commissioner has agreed to accept such undertaking. NOW THIS AGREEMENT WITNESSES that in consideration of the premises, the Bank at the request of the contractors (hereby testified) UNDERTAKES WITH the Commissioner to pay to the Commissioner upon demand in writing, whenever required by him, from time to time, so to do, a sum not exceeding in the whole Rs.----- (Rupees-----) under the terms of the said tender and/or the contract. The B.G. is valid upto-----

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



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

IN WITNESS WHEREOF

WITNESS (1) -----

Name and -----

Address -----

-----

WITNESS (2) -----

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

Address -----

-----

the Bank and the said Messrs-----

----- (Name of the bank)

WITNESS (1) -----

Name and -----

Address -----

-----

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

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

Address -----

-----

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

## **8 Annexure II: Instructions and Technical Bid Document Formats**

### **8.1 General Instructions**

Bidders have to submit a very structured and organized technical bid, which will be analysed by the Evaluation Committee for different compliances with regard to the requirements of the project. Since the cut-off marks for Technical bid Score is 70, the quality and completeness of the information submitted by the Bidder is of utmost importance.

Bidder is expected to divide its Bid in following sections / documents:

#### **A. Bidder's Competence to Execute the Project**

This document should bring about the capability of the firm to execute this project. Some of the required documents are as follows:

1. Financial Capability of the Bidder in required formats and supporting documents
2. Experience of Bidder in implementation or post implementation support projects in required formats
3. Experience of Bidder in execution of projects (IT Audit/ Process Audit / Compliance audit) in Urban Local Bodies / Public Sector Companies in India in required format
4. Experience of Bidder in executing implementation or post implementation support projects with Urban Local Bodies in India

#### **B. Technical Solution Proposed for the Project**

Broad areas to be covered in the Technical Solution documentation are given below:

1. Mapping of features as per the requirements specified in the bid document
2. Describe the proposed Technical Solution in a structured manner. Following should be captured in the same:
  - a. Strength of the Bidder to provide services including examples or case-studies of similar facilities provided for other clients
3. Approach and Methodology for Management of SLA Requirements specified in the bid. Bidder is required to clearly articulate how the SLA requirements would be adhered to.
4. Detailed Project Plan with timelines, resource allocation, milestones etc. for execution of the project

All above mentioned documents shall have an index page with page numbers specified for all the key information / headers.

## 8.2 Format to Share Project Details

Name of the Project	
General Information	
Client for which the project was executed	
Name of the client contact person(s)	
Designation of client contact person(s)	
Contact details of the client contact person(s)	
Project Details	
Description of the project	
Scope of work of the Bidder	
Deliverables of the Bidder	
Technologies used	
Current Status of the project	
Other Details	
Total cost of the project	
Total cost of the services provided by the Bidder	
Duration of the project (number of months, start date, completion date, current status)	
Other Relevant Information	
Mandatory Supporting Documents:	
<ul style="list-style-type: none"> <li>• Work order / Purchase order / Contract for the project</li> </ul>	

Note: The Bidder is required to use above format for all the projects referenced by the Bidder for the pre-qualification criteria and technical bid evaluation.

### 8.3 Details of Manpower Resources Proposed

#	Name of the Proposed Auditor	Professional Qualification	Certifications /Accreditations	IT Expertise in terms of years and areas of expertise	Total Relevant Experience for the proposed position (in years)

### 8.4 CV of the Proposed Key Manpower

1.	Name of the Staff	
2.	Current Designation in the Organisation	
3.	Proposed Role in the Project	
4.	Proposed Responsibilities in the Project	
5.	Date of Birth	
6.	Education	<ul style="list-style-type: none"> <li>▪ Degree / Diploma, College, University, Year of Passing</li> <li>▪ Degree / Diploma, College, University, Year of Passing</li> </ul>
7.	Summary of Key Training and Certifications	

8.	Language Proficiency	Language	Reading	Writing	Speaking
9.	Employment Record (For the total relevant experience)	From / To:			
		Employer:			
		Position Held:			
		From / To:			
		Employer:			
		Position Held:			
		From / To:			
		Employer:			
		Position Held:			
10.	Total No. Of Years of Work Experience				
11.	Total No. Of Years of Experience for the Role proposed				
12.	Highlights of relevant assignments handled and significant accomplishments (Use following	Name of assignment or project:			
		Year:			
		Location:			
		Client:			
		Main project features:			

	format for each project)	Positions held:		
		Activities performed:		

**9 Annexure III: Commercial Bid Formats****9.1 Commercial Bid Cover Letter**

Date: dd/mm/yyyy

To

<Insert complete postal address>

**Sub :** <Insert project/bid name>

**Ref :** Bid No: <No>      Dated <DD/MM/YYYY>

Dear Sir,

We, the undersigned Bidders, having read and examined in detail all the bidding documents in respect of **Implementation of IT Audit at Municipal Corporation of Greater Mumbai** do hereby propose to provide services as specified in the bid referred above.

**1. PRICE AND VALIDITY**

- All the prices mentioned in our bid are in accordance with the terms as specified in the bid documents. All the prices and other terms and conditions of this bid are valid for a period of 180 calendar days from the date of opening of the Bids.
- We hereby confirm that our bid prices include all taxes. Taxes are quoted separately under relevant sections, as specified in the bid formats.
- We have studied the clause relating to Indian Income Tax and hereby declare that if any income tax, surcharge on Income Tax, Professional and any other Corporate Tax in altered under the law, we shall pay the same.

**2. UNIT RATES**

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

### **3. DEVIATIONS**

We declare that all the services shall be performed strictly in accordance with the bid documents and there are no deviations.

### **4. QUALIFYING DATA**

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

### **5. BID PRICE**

We declare that our Bid Price is for the entire scope of the work as specified in the bid document. These prices are indicated in the subsequent sub-sections of this Section.

### **6. CONTRACT PERFORMANCE GUARANTEE BOND**

We hereby declare that in case the contract is awarded to us, we shall submit the contract Performance Bank Guarantee in the form prescribed in the bid.

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

We understand that our bid is binding on us and that you are not bound to accept a bid you receive. We confirm that no Technical deviations are attached here with this commercial offer.

Thanking you,

Yours faithfully,

Signatory)

(Signature of the Authorised

Name

Designation

Seal.



Date:

Place:

Business Address:

## 9.2 Commercial Bid Format and Instructions

1. Bidder is required to score a minimum of 70% before commercial bid opening.
2. Bidders are required to quote the rates of items of work inclusive of all taxes in the commercial offer of e-tendering system of MCGM, as there is no provision for quoting for taxes separately.
3. The Bidder has to quote the rate in the BoQ available online via e-Tendering and should not be filled in physically. The instructions for online e-tendering have been illustrated clearly on the web link – [User Manuals](#)
4. Details to be filled up for price bid for different type of Audit activity are as follows:

### Section A Preliminary Audit

Preliminary Audit (PA)					
Sr. No.	Item of Work	Quantity	Unit of Measurement	Unit Cost (Inclusive of taxes)	Total Cost (Inclusive of taxes)
1	<b>IT Infrastructure Audit of WDC</b>				
1.1	IT infrastructure in WDC (Non-IT)	91	Nos.		
1.2	Network - Architecture, Performance and Security review	38	Nos.		
1.3	VA for Host / Servers / Network	83	Nos.		
1.4	Penetration Testing for Host / Servers / Network	35	Nos.		
1.5	Audit of Network, Backup and Security Devices	51	Nos.		
1.6	Server, Operating System Audit	42	Nos.		
1.7	Infrastructure Hardware Audit	37	Nos.		
1.8	Endpoints at WDC Area	50	Nos.		

2	<b>Audit of Cloud</b>				
2.1	IT infrastructure in Cloud (Non-IT)	NA	Nos.		
2.2	Network - Architecture, Performance and Security review	8	Nos.		
2.3	VA for Host / Servers / Network	238	Nos.		
2.4	Penetration Testing for Host / Servers / Network	175	Nos.		
2.5	Audit of Network, Backup and Security Devices	347	Nos.		
2.6	Server, Operating System Audit	216	Nos.		
2.7	Infrastructure Hardware Audit (Physical Servers)	18	Nos.		
3	Digital Forensics Readiness Assessment (For Complete MCGM Applications and systems)	1	No.		
4	Process Review	20	Nos.		
5	<b>SAP applications</b>				
5.1	SAP SRM	1	Nos.		
5.2	SAP CRM	1	Nos.		
5.3	SAP MM	1	Nos.		
5.4	SAP PS	1	Nos.		
5.5	SAP HR	1	Nos.		
5.6	SAP FICO	1	Nos.		
5.7	SAP BI	1	Nos.		
5.8	SAP RE	1	Nos.		
5.9	SAP Fleet Management	1	Nos.		
5.10	SAP Technical Control/ BASIS	1	Nos.		
5.11	SAP EP	1	Nos.		

5.1 2	SAP IS Utility	1	Nos.		
6	<b>Non-SAP Applications</b>				
6.1	CVS	1	Nos.		
6.2	AQUA	1	Nos.		
6.3	GIS DP	1	Nos.		
6.4	GIS SO	1	Nos.		
6.5	AutoDCR	1	Nos.		
6.6	eOffice	1	Nos.		
	GIS	1	No.		
6.8	GIS A&C	1	Nos.		
6.9	Rain Gauge	1	Nos.		
6.1 0	Command & Control	1	Nos.		
6.1 1	VTMS	1	Nos.		
6.1 2	DMS	1	Nos.		
6.1 3	LMS	1	Nos.		
6.1 6	HMIS	1	Nos.		
6.1 7	email	1	Nos.		
7	Android based mobile applications	1	Nos.		
8	IOS based mobile applications	1	Nos.		
9	IT Audit for locations	3	Nos.		
	<b>Section A Total</b>				

**Section B Compliance Review:**

<b>Compliance Review (CA)</b>					
<b>Sr. No.</b>	<b>Item of Work</b>	<b>Quantity</b>	<b>Unit of Measurement</b>	<b>Unit Cost (Inclusive of taxes)</b>	<b>Total Cost (Inclusive of taxes)</b>
<b>1</b>	<b>IT Infrastructure Audit of WDC</b>				
1.1	IT infrastructure in WDC (Non-IT)	91	Nos.		
1.2	Network - Architecture, Performance and Security review	38	Nos.		
1.3	VA for Host / Servers / Network	83	Nos.		
1.4	Penetration Testing for Host / Servers / Network	35	Nos.		
1.5	Audit of Network, Backup and Security Devices	51	Nos.		
1.6	Server, Operating System Audit	42	Nos.		
1.7	Infrastructure Hardware Audit	37	Nos.		
1.8	Endpoints at WDC Area	50	Nos.		
<b>2</b>	<b>Audit of Cloud</b>				
2.1	IT infrastructure in Cloud (Non-IT)	NA	Nos.		
2.2	Network - Architecture, Performance and Security review	8	Nos.		
2.3	VA for Host / Servers / Network	238	Nos.		
2.4	Penetration Testing for Host / Servers / Network	175	Nos.		

2.5	Audit of Network, Backup and Security Devices	347	Nos.		
2.6	Server, Operating System Audit	216	Nos.		
2.7	Infrastructure Hardware Audit	18	Nos.		
3	Digital Forensics Readiness Assessment (For Complete MCGM Applications and systems)	1	No.		
4	Process Review	20	Nos.		
5	<b>SAP applications</b>				
5.1	SAP SRM	1	Nos.		
5.2	SAP CRM	1	Nos.		
5.3	SAP MM	1	Nos.		
5.4	SAP PS	1	Nos.		
5.5	SAP HR	1	Nos.		
5.6	SAP FICO	1	Nos.		
5.7	SAP BI	1	Nos.		
5.8	SAP RE	1	Nos.		
5.9	SAP Fleet Management	1	Nos.		
5.10	SAP Technical Control/ BASIS	1	Nos.		
5.11	SAP EP	1	Nos.		
5.12	SAP IS Utility	1	Nos.		
6	<b>Non-SAP Applications</b>				
6.1	CVS	1	Nos.		
6.2	AQUA	1	Nos.		
6.3	GIS DP	1	Nos.		
6.4	GIS SO	1	Nos.		
6.5	AutoDCR	1	Nos.		

6.6	eOffice	1	Nos.		
	GIS	1	No.		
6.8	GIS A&C	1	Nos.		
6.9	Rain Gauge	1	Nos.		
6.10	Command & Control	1	Nos.		
6.11	VTMS	1	Nos.		
6.12	DMS	1	Nos.		
6.13	LMS	1	Nos.		
6.16	HMIS	1	Nos.		
6.17	email	1	Nos.		
7	Android based mobile applications	1	Nos.		
8	IOS based mobile applications	1	Nos.		
9	IT Audit for locations	3	Nos.		
	<b>Section B Total</b>				

**Note:**

- MCGM reserves the right to increase or decrease resources during the tenure of the contract; an intimation of the same would be made to the selected agency in writing.
- Quantity mentioned in the commercial bid format may at actuals. MCGM may add the quantities upto 25% of each line items or drop / replace any line item during the tenure of the contract as mentioned in the Commercial bid format.
- MCGM shall make payment on individual line items as mentioned in Section A and Section B considering the delivery and successful execution of the scope of work.

The fees shall be **inclusive** of GST, Income Tax, duties, fees, levies, charges, and commissions as applicable under the relevant Laws of India. Should there be a change in applicable taxes, the actual taxes on the date of billing would prevail.

**Note:**

1. The Bidder should submit only the 'Summary of the Commercial Format' on <https://portal.mcgm.gov.in> and the detailed commercial bid should be submitted within 2 days of the opening of commercial Packet. The formats for detailed commercial bids to be as per formats defined in this RFP.
2. The bidders may visit the site and obtain additional information at their own cost and responsibility.
3. The Bidder will quote for the resources after considering all the relevant costs required to accomplish the necessary scope, details of which are mentioned in the Scope of Work section of this Bid document.
4. It is mandatory for the successful bidder to open a bank account in any of the banks approved by MCGM (Specified in Annexure IV of the bid document) for easy and quick payments. All payments under the contract will be made only in this bank account through Electronic Clearing System/RTGS/NEFT/CBS.
5. A Project Implementation Committee (PIC) will be constituted which will be responsible for monitoring the performance of the Selected Agency and recommend for the payment.
6. The Bidder should submit only the 'Summary of the Commercial Format' on <https://portal.mcgm.gov.in> and the detailed commercial bid should be submitted within 2 days of the opening of commercial Packet. The formats for detailed commercial bids to be as per formats defined in this RFP.
7. The bidders may visit the site and obtain additional information at their own cost and responsibility.
8. If the Selected Agency is liable for any penalty/liquidated damages as per the SLA (refer to the section no. 7 of this agreement), the same shall be adjusted from payments due to the Selected Agency as per payment terms.
9. MCGM reserves the right to scale up and scale down resources based on requirements. Any line items may be removed from the scope based on MCGM's discretion.
10. All the prices are to be entered in Indian Rupees ONLY.
11. The allocated PR Assistants of the Selected Agency to provide services of different departments/ accounts can be interchanged as per the requirement of the MCGM and in this case the order of the Director (IT) will be final. Also, it is to be mentioned that Vendor is strictly



not allowed for resource interchange among different departments/ accounts without MCGM permission.

12. Prices indicated in the schedules shall be inclusive of all taxes, Levies, duties etc. It is mandatory to provide breakup of all Taxes, Duties and Levies wherever asked for.
13. During the payment stage, MCGM reserves the right to ask the Bidder to submit proof of payment against any of the taxes, duties, levies indicated.
14. The Bidder needs to account for all Out of Pocket expenses due to Boarding, Lodging and other related items. No additional/separate payment shall be made regarding the same.
15. For the purpose of evaluation of Commercial Bids, MCGM shall make appropriate assumptions to arrive at a common bid price for all the Bidders. This however shall have no co-relation with the Contract value or actual payment to be made to the Bidder.
16. The Contract Price shall be firm and not subject to any alteration.
17. The Selected Agency should be deemed to have satisfied itself as to the correctness and sufficiency of the contract price, which shall, except as otherwise provided for in the contract, cover all its obligations under the contract.
18. Wherever present, the items mentioned as Lump Sum in above table will have quantity as 1 in the BoQ available online via e-tendering. However, the bidder should consider the same as Lump Sum and submit the commercials.
19. All payments shall be made for the corresponding goods or services actually delivered, installed, or operationally accepted, per the Contract Implementation Schedule, at unit prices and in the currencies specified in the Commercial Bids.

### **9.3 Commercial Proposal Format & Instruction**

The **least** rate will decide the L1 vendor.

1. The total mentioned above will be considered as final bid price by bidder for commercial evaluation.
2. The rate quoted for the project must be inclusive of any out of pocket and any other incidental expenses.
3. The rate quoted shall be inclusive of cost of detailed scope of work of the RFP document.
4. The quoted rates shall be inclusive of all operational costs to render services as per the Scope.

Note: -

1. The bidders may visit the site and obtain additional information at their own cost and responsibility.
2. All the prices are to be entered in Indian Rupees ONLY.
3. The Bidder needs to account for all Out of Pocket expenses due to Boarding, Lodging and other related items.
4. Prices indicated in the schedules shall be inclusive of all taxes, Levies, duties etc. It is mandatory to provide breakup of all Taxes, Duties and Levies wherever asked for. During the payment stage, MCGM reserves the right to ask the Bidder to submit proof of payment against any of the taxes, duties, levies indicated.
5. For the purpose of evaluation of Commercial Bids, MCGM shall make appropriate assumptions to arrive at a common bid price for all the Bidders. This however shall have no co-relation with the Contract value or actual payment to be made to the Bidder.
6. The Contract Price shall be a firm lump sum not subject to any alteration.
7. The selected agency shall be deemed to have satisfied itself as to the correctness and sufficiency of the contract price, which shall, except as otherwise provided for in the contract, cover all its obligations under the contract.

**9.4 Commercial Format (Online)**

(to be uploaded in “C” folder online)

Name \_\_\_\_\_ of \_\_\_\_\_ Work: \_\_\_\_\_

Sr. No.	Item Description	Amount Incl. of all taxes & duties	Bidder to indicate the amount of applicable taxes/duties								
			CGST		SGST		IGST		Other Taxes/duties (if any)		Total Amount of Taxes
			%	Amount	%	Amount	%	Amount	%	Amount	
Grand Total											

**10 Annexure IV: List of Approved Banks**

The Earnest Money Deposit (EMD) / Bank Guarantee (PBG) issued by branches of approved Banks beyond Kalyan and Virar can be accepted only if the said EMD / PBG is countersigned by the Manager of a Branch of the same Bank within the Mumbai City limit categorically endorsing thereon that the said EMD / BG is binding on the endorsing Branch of the Bank within Mumbai limits and is liable to be enforced against the said Branch of the Bank in case of default by the Selected Agency furnishing the Banker's guarantee.

<b>State Bank of India and its subsidiary banks.</b>		
1. State Bank of India.		
<b>Nationalized Banks.</b>		
2. Allahabad Bank.	3. Andhra Bank.	4. Bank of Baroda.
5. Bank of India.	6. Bank of Maharashtra.	7. Canara Bank.
8. Central Bank of India.	9. Corporation Bank.	10. Indian Bank.
11. Indian Overseas Bank.	12. Oriental Bank of Commerce.	13. Punjab National Bank.
14. Punjab and Sind Bank.	15. Syndicate Bank.	16. UCO Bank.
17. Union Bank of India.	18. United Bank of India.	
<b>Other Public Sector Banks.</b>		
19. Industrial Development Bank of India (IDBI)		
<b>Private Sector Banks.</b>		
20. Axis Bank Ltd.	21. Bank of Rajasthan Ltd.	22. Catholic Syrian Bank Ltd.
23. City Union Bank Ltd.	24. Development Credit Bank Ltd.	25. Dhanalakshmi Bank Ltd.
26. Federal Bank Ltd.	27. HDFC Bank Ltd.	28. ICICI Bank Ltd.
29. IndusInd Bank Ltd.	30. ING Vysya Bank Ltd.	31. Jammu and Kashmir Bank Ltd.

32. Karnataka Bank Ltd.	33. Karur Vysya Bank Ltd.	34. Kotak Mahindra Bank Ltd.
35. Lakshmi Vilas Bank Ltd.	36. Nainital Bank Ltd.	37. Ratnakar Bank Ltd.
38. SBI Commercial International Bank Ltd.	39. South Indian Bank Ltd.	40. Tamil land Mercantile Bank Ltd.
41. Yes Bank Ltd.		
<b>Scheduled Urban Co-op. Banks Licensed to issued Bankers Guarantee.</b>		
42. Abhyudaya Co-Op. Bank Ltd.	43. Bassein Catholic Co-Op. Bank Ltd.	44. Bharat Co-Op. Bank Ltd.
45. Bombay Mercantile Co-Op. Bank Ltd.	46. Citizen Credit Co-Op. Bank Ltd.	47. Dombivli Nagari Sahakari Bank Ltd.
48. Greater Mumbai Co-Op. Bank Ltd.	49. JanakalyanSahakari Bank Ltd.	50. Janata Sahakari Bank Ltd.
51. Kalyan Janata Sahakari Bank Ltd.	52. Kapol Co-Op. Bank Ltd.	53. Mahanagar Co-Op. Bank Ltd.
54. Mumbai District Central Co-Op. Bank Ltd.	55. NKGSB Co-Op. Bank Ltd.	56. New India Co-Op. Bank Ltd.
57. Parsik Janata Sahakari Bank Ltd.	58. Punjab & Maharashtra Co-Op. Bank Ltd.	59. Rupee Co-Op. Bank Ltd.
60. Sangli Urban Co-Op. Bank Ltd.	61. Saraswat Co-Op. Bank Ltd.	62. Thane Bharat Sahakari Bank Ltd.
63. Thane Janata Sahakri Bank Ltd.	64. The Cosmos Co-Op. Bank Ltd.	65. The ShamraoVitthal Co-Op. Bank Ltd.
66. The Zoroastrian Co-Op. Bank.		
<b>State Co-op. Banks.</b>		
67. The Maharashtra State Co-Op. Bank.		
<b>Foreign Banks.</b>		

68. ABN Amro Bank N. V.	69. Abu Dhabi Commercial Bank Ltd.	70. American Express Banking Corporation.
71. Antwerp Diamond Bank N. V.	72. Arab Bangladesh Bank.	73. Bank International Indonesia.
74. Bank of America.	75. Bank of Bahrain and Kuwait BSC.	76. Bank of Ceylon.
77. Bank of Nova Scotia.	78. Bank of Tokyo-Mitsubishi Ltd.	79. Barclays Bank Plc.
80. BNP Paribas.	81. China Trust Commercial Bank.	82. Shinhan Bank.
83. Citi Bank N.A.	84. Calyon Bank.	85. Deutsche Bank.
86. DBS Bank Ltd.	87. The Hongkong and Shanghai Banking Corporation Ltd. (HSBC)	88. J.P. Morgan Chase Bank N.A.
89. Krung Thai Bank Public Company Ltd.	90. Mashreq Bank psc.	91. Mizuho Corporate Bank Ltd.
92. Oman International Bank S.A.O.G.	93. Societe Generale.	94. Sonali Bank.
95. Standard Chartered Bank.	96. State Bank of Mauritius Ltd.	

**11 Annexure V: Authorization Letter for Attending Bid Opening**

(to be provided on the letter head of Bidder)

No.....

Date.....

To

The.....

Municipal Corporation of Greater Mumbai,  
Mumbai.

Sub: Bid No..... due date.....

Sir,

We hereby authorize Mr./Ms. ....as our authorized representative, to  
represent us at: -

- Bid Opening on..... At..... A.M. /P.M.

Kindly permit him/her to attend the same.

Yours faithfully,

Signature:

Name of signatory:

Designation:

Rubber Stamp:

**12 Annexure VI: Draft Contract Agreement**

**Stamp duty Rs. 500/- up to 10,00,000/- + 0.01% of the amount above Rs. 10 lakh subjects to maximum of 25 lakhs.**

Bid No.: \_\_\_\_\_

Sanction No. & Date: \_\_\_\_\_

Contract Value: \_\_\_\_\_

This Contract Agreement, hereinafter referred to as “**CA**” is made this \_\_\_\_ day of \_\_\_\_\_ 20\_\_ at [office address]

BETWEEN

<Head of Department>, Municipal Corporation of Greater Mumbai, Maharashtra State, (which term or expression, unless excluded by or repugnant to the subject or context, shall mean and include its successors-in office and assigns) of the First Part (which term or expression, unless excluded by or repugnant to the subject or context, shall mean and include its successors-in office and assigns) of the First Part

AND

M/s \_\_\_\_\_, a company registered <Select as under The Companies Act, 1956 or Partnership Act, 1932 as applicable> having its registered office at \_\_\_\_\_ and place of business at \_\_\_\_\_, hereinafter referred to as “**Selected Agency**” (which term or expression, unless excluded by or repugnant to the subject or context, shall mean and include its successors and permitted assigns) of the Second Part

Each individually a “Party” hereto and collectively the “Parties”

And Whereas MCGM intends to provide convenient and speedy services using Information and Communication Technologies (ICT) to its officials and has published the bid to seek services <include scope of project and bid name> till the end of the contract period;



And whereas M/s. ----- has submitted its bid to <**Project Name**>for MCGM;

And whereas MCGM and M/s. ----- have decided to enter into this Agreement on the terms and conditions stipulated hereinafter.

NOW, THEREFORE, in consideration of the premises covenants and promises contained herein and other good and valuable considerations, the receipt and adequacy of which is hereby acknowledged, the parties intending to be bound legally, IT IS HEREBY AGREED between the Parties as follows:

### **12.1 Definitions, Interpretations and Other Terms**

- a. **Bid** means the bid process conducted by MCGM and the technical and commercial bids submitted by the successful Bidder, along with the subsequent clarifications and undertakings, if any;
- b. The **“Contract”** shall mean the tender and acceptance thereof and the formal Agreement if any, executed between the Bidder, Commissioner and the Corporation together with the documents referred to therein including these conditions and appendices and any special conditions, the specifications, designs, drawings, price schedules, bills of quantities and schedule of rates. All these documents taken together shall be deemed to form one Contract and shall be complementary to one another.
- c. The **“Bidder”** shall mean a person or corporate body who has desired to submit Bid to carry out the Works, including routine maintenance till the tender process is concluded.
- d. **“Arbitrator”** means the person or persons appointed by agreement between MCGM and the Bidder to make a decision on or to settle any dispute or difference between the MCGM and the Bidder referred to him or her by the parties pursuant to General Conditions of Contract amended up to date.
- e. **“Contract Cost”** means the Contract Sum plus Price Variation. This cost shall be included in the letter of acceptance.
- f. **“Excepted risks”** are risks due to riots (otherwise than among Bidder’s employees) and civil commotion (in so far as both these are uninsurable), war (whether declared or not), invasion, act of foreign enemies, hostilities, civil war, rebellion, revolution,

insurrection, military or usurped power, any act of government, damage from aircraft, acts of god, such as earthquake, lightning and unprecedented floods and other causes over which the Bidder has no control and accepted as such by the Commissioner or causes solely due to use or occupation by the Municipal Corporation of the works in respect of which a certificate of completion has been issued or a cause solely due to faulty municipal design of work.

- g. The **“Corporation”** or the **“Municipal Corporation”** shall mean the Municipal Corporation of Greater Mumbai, constituted under the M.M.C. Act 1888 as amended up to date.
- h. The **“Annexure”** referred to in these conditions shall mean the relevant annexure appended to the tender papers issued by the Municipal Corporation.
- i. The **“Works”** shall mean the Permanent Works and the Temporary Works or either of them as appropriate to be executed in accordance with the contract or part(s) thereof, as the case may be and shall include all extra or additional, altered or substituted works as required for performance.
- j. **“Temporary Works”** shall mean all Temporary Works of every kind required in or about execution, completion or maintenance of the work also Temporary Works are works designed, constructed, installed, and removed by the Selected Agency that are needed for construction or installation of the Works of the contract as found necessary as per suggestion of the MCGM.
- k. **“Permanent Works”** means the permanent works to be executed and installation of machineries in accordance with the Contract at specified required site and location.
- l. **“Drawings”** means all the drawings, calculations and technical information of a like nature provided by the MCGM to the Selected Agency under the Contract and all drawings, calculations, samples, patterns, models, operation & maintenance manual and other technical information of like nature submitted by the Selected Agency and approved by the MCGM.
- m. **“Approved”** shall mean approved in writing including subsequent confirmation of previous verbal approval and “approval” shall mean approval in writing including as aforesaid.

- n. **“Specification”** means the specification referred to in the tender and any modification thereof or addition or deduction thereto as may from time to time be furnished or approved in writing by the MCGM.
- o. **“Tender”** means the Bidder’s priced offer to the MCGM for the execution and completion of the Works and the remedying of any defects therein in accordance with the provision of the Contract, as accepted by the Letter of Acceptance.
- p. **“Commencement Date”** means the date upon which the Bidder receives the notice to commence, issued by the MCGM
- q. **“Time for Completion”** means the time for completing the execution of and passing the Tests on Completion of the Works or any Section or part thereof as stated in the Contract calculated from the Commencement Date.
- r. **“Certificate of Taking-Over/ Take-over Certificate”** shall mean the certificate issued by MCGM after completion of Works in all respects.
- s. **“Letter of Acceptance”** means the letter of formal acceptance, signed by MCGM, of the Letter of Bid, including any annexed memoranda comprising agreements between and signed by both Parties. If there is no such letter of acceptance, the expression “Letter of Acceptance” means the Contract Agreement and the date of issuing or receiving the Letter of Acceptance means the date of signing the Contract Agreement.
- t. **“Cost”** means all expenditure properly incurred or to be incurred whether on or off the site including overheads and other charges properly allocable thereto but does not include any allowance for profit.
- u. **Confidential Information** means all information including MCGM Data (whether in written, oral, electronic or other format) which relates to the technical, financial, business affairs, customers, suppliers, products, developments, operations, processes, data, trade secrets, design rights, know-how and personnel of each Party and its affiliates which is disclosed to or otherwise learned by the other Party in the course of or in connection with this CA (including without limitation such information received during negotiations, location visits and meetings in connection with this CA);
- v. **Customers** mean all citizens and business organization and users who use the MCGM services.

- w. **Deliverables** means all the activities related to the setting up and operations of the infrastructure, technical documents, Software Applications, customized Source Codes, as defined in the bid and subsequent Corrigendum (if any), based on which the technical bid and commercial bid was submitted by the Bidder and as required as per this CA;
- x. **Effective Date** means the date on which the Purchase Order or Letter of Intent is issued to Selected Agency;
- y. **CA** means this Contract Agreement, together with the recitals and all schedules and the contents, requirements, specifications and standards of the bid (as may be amended, supplemented or modified in accordance with the provisions hereof) and the bid. **In the event of a conflict between this CA and the Schedules, the terms of the CA shall prevail; with overriding effect;**
- z. **Performance Security** means the irrevocable and unconditional Bank Guarantee provided by the Selected Agency from by any of the approved banks as specified in Annexure of this RFP document in favour of “Municipal Corporation of Greater Mumbai” for an amount equivalent to 10% of the total contract value i.e. Rs.....(Rupees.....only);
- aa. **Proprietary Information** means processes, methodologies and technical and business information, including drawings, designs, formulae, flow charts, data and computer programs already owned/licensed by either Party or granted by third parties to a Party hereto prior/ subsequent to the execution of this CA;
- bb. **Required Consents** means the written consents, clearances and licenses, rights and other authorizations as may be required to be obtained by the Selected Agency, for all tasks/activities/software/hardware and communication technology for this project; from all the concerned departments/agencies, etc. as the case may be.
- cc. **Bid** means the bid document released vide bid document number mentioned in RFP and include all clarifications/addendums, explanations and amendments issued by the Corporation in respect thereof;
- dd. **Service Level(s)** means the performance standards, which will apply, to the services delivered through the Software Application and hardware implemented by the Selected Agency.

- ee. **Service Level Requirement(s)** means the timelines and the quality levels to be adhered to by the Selected Agency for delivering various services under the contract;
- ff. **Services** means the content and services delivered and to be delivered to the customers or the offices of MCGM by the Selected Agency, and includes but not limited to the services specified in the bid document or as may be specified and incorporated in the subsequent Agreement/s under Contract Agreement.
- gg. **Users** means the departmental staffs or any other MCGM officials having access to application including its Implementation Agencies, technology vendors, corporations and agencies and their employees, as the context admits or requires.
- hh. **“Day”** means Calendar day.
- ii. **“Month”** means Calendar month of the Gregorian calendar.
- jj. **“GCC”** means General Conditions of Contract.
- kk. **“Foreign Currency”** means currency of a country other than that in which the works are to be located, approved by Govt of INDIA/Reserve Bank of INDIA.
- ll. **“Writing”** means any hand written, type-written, or printed communication including telex and facsimile transmission, electronic and digital media.
- mm. **“Country”** means the country in which the Site is located.
- nn. **“Variation”** means a change to the:-
  - I. Specification and /or Drawings (if any) which is instructed by the MCGM.
  - II. Scope in the Contract which is instructed by the MCGM.
  - III. Price in the Contract which is instructed by the MCGM
- oo. **“Specification”** shall mean the specification referred to in the tender and any modification thereof or addition or deduction thereto as may from time to time be furnished or approved in writing by the MCGM.
- pp. **The Start Date/Commencement Date** is given in the Contract Data. It is the date when the Selected Agency shall commence execution of the Works. It does not necessarily coincide with any of the Site Possession Dates.

## 12.2 Interpretations

- a. References to any statute or statutory provision include a reference to that statute or statutory provision as from time to time amended, extended, re-enacted or consolidated and to all statutory instruments made pursuant to it;

- b. Words denoting the singular shall include the plural and vice-versa and words denoting persons shall include firms and corporations and vice versa;
- c. Unless otherwise expressly stated, the words “herein”, “hereof”, “hereunder” and similar words refer to this CA as a whole and not to any particular Article, Schedule. The term Articles, refers to Articles of this CA. The words “include” and “including” shall not be construed as terms of limitation. The words “day” and “month” mean “calendar day” and “calendar month” unless otherwise stated. The words “writing” and “written” mean “in documented form”, whether electronic or hard copy, unless otherwise stated;
- d. The headings and use of bold type in this CA are for convenience only and shall not affect the interpretation of any provision of this CA;
- e. The Schedules to this CA form an integral part of this CA and will be in full force and effect as though they were expressly set out in the body of this CA;
- f. Reference at any time to any agreement, deed, instrument, license or document of any description shall be construed as reference to such agreement, deed, instrument, license or other document as the same may be amended, varied, supplemented, modified or suspended at the time of such reference;
- g. References “roll out” includes, unless the context otherwise requires, design, development, implementation, engineering, procurement, delivery, transportation, installation, processing, fabrication, acceptance testing, certification, commissioning and other activities incidental to the construction or roll out, and “construct” or “roll out” shall be construed accordingly;
- h. Any word or expression used in this CA shall, unless defined or construed in this CA, bear its ordinary English language meaning;
- i. The damages payable by a Party to the other Party as set forth in this CA, whether on per diem basis or otherwise, are mutually agreed genuine pre-estimated loss and liquidated damages likely to be suffered and incurred by the Party entitled to receive the same and are not by way of penalties;
- j. This CA shall operate as a legally binding agreement specifying the master terms, which apply to the Parties under this agreement and to the provision of the services by the Selected Agency;

- k. The Corporation may nominate a technically competent agency/individual(s) for conducting acceptance testing and certification of the various requisite infrastructure/service to ensure a smooth, trouble free and efficient functioning of the Scheme or carry out these tasks itself;
- l. The agency/individual nominated by the Corporation can engage professional organizations for conducting specific tests on the software, hardware, networking, security and all other aspects;
- m. The agency/individual will establish appropriate processes for notifying the Selected Agency of any deviations from the norms, standards or guidelines at the earliest instance after taking cognizance of the same to enable the Selected Agency to take corrective action;
- n. Such an involvement of and guidance by the agency/person will not, however, absolve the Selected Agency of the fundamental responsibility of designing, installing, testing and commissioning the application and the infrastructure for efficient and effective delivery of services as contemplated under this bid.
- o. The following documents forming this Agreement are to be taken as mutually explanatory of one another:
  - i. This Agreement;
  - ii. Purchase Order or Letter of Intent issued by MCGM to the successful Bidder and
  - iii. Clarification and Corrigendum Documents published by MCGM subsequent to the bid for this work
  - iv. Bid Document of MCGM for this work
  - v. Detail Commercial bid of the Selected Agency accepted by MCGM
  - vi. Successful Bidder's 'Technical Bid' submitted in response to the bid and responses/clarifications provided in response to queries raised by BEC

### **12.3 Term of the Contract Agreement**

- 1. The term of this CA shall be a period of one year from the date of issue of LOA/LOI. This includes the time required for Implementation and Operations and Maintenance Support.

2. In the event of implementation period getting extended beyond the stipulated time, for reasons not attributable to the Selected Agency, MCGM reserves the right to extend the term of the Agreement by a suitable period with mutual consensus to allow validity of contract from the date of operational acceptance.

#### **12.4 MCGM's Decision**

Except where otherwise specifically stated, the MCGM representative will decide contractual matters between MCGM and the Bidder in the role representing the MCGM. However, if MCGM representative is required under the rules and regulations and orders of the MCGM to obtain prior approval of some other authorities for specific actions, he will so obtain the approval, before Communicating his decision to the Bidder.

Except as expressly stated in the Contract, MCGM representative shall not have any authority to relieve the Contractor of any of his obligations under the contract.

#### **12.5 Delegation**

MCGM representative, with the approval of the MCGM Authority, may delegate any of his duties and responsibilities to other person(s), except to the Adjudicator, after notifying the Bidder, and may cancel any delegation after notifying the Bidder.

#### **12.6 Communication**

All certificates, notices or instructions to be given to the Bidder by MCGM shall be sent on the address / Email Address or contact details given by the Bidder of Bid. The address and contact details for communication with the MCGM shall be as per the details given in Contract Data. Communications between parties that are referred to in the conditions shall be in writing. The Notice sent by facsimile (fax) or other electronic means shall be effective on confirmation of the transmission. The Notice sent by Registered post or Speed post shall be effective on delivery or at the expiry of the normal delivery period as undertaken by the postal service.

#### **12.7 Other Bidders**

The Bidder shall cooperate and share the Site with other Bidder, public authorities, utilities, and the MCGM between the dates given in the Schedule of Other Bidder, as referred to in the Contract Data. The Bidder shall also provide facilities and services for them as described

---



in the Schedule. The MCGM may modify the Schedule of Other Bidder and shall notify the Bidder of any such modification.

## **12.8 Personnel**

The Selected Agency's personnel shall appropriately be qualified, skilled and experienced in their respective trades or occupations. MCGM shall have authority to remove, or cause to be removed, any person employed on the site or works, who carries out duties incompetently or negligently.

If MCGM asks the Selected Agency to remove a person who is a member of the Selected Agency's staff or work force, stating the reasons, the Selected Agency shall ensure that the person leaves the Site within seven days and has no further connection with the Works in the Contract. Selected agency has to provide replacement of that staff.

## **12.9 MCGM's and Selected Agency's Risks**

The MCGM carries the risks which this Contract states are MCGM's risks, and the Selected Agency carries the risks which this Contract states are Selected Agency's risks.

## **12.10 MCGM's Risks**

The MCGM is responsible for the excepted risks which are (a) in so far as they directly affect the execution of the Works, the risks of war, invasion, act of foreign enemies, rebellion, revolution, insurrection or military or usurped power, civil war, riot, commotion or disorder (unless restricted to the Selected Agency's employees) and contamination from any nuclear fuel or nuclear waste or radioactive toxic explosive, or (b) a cause due solely to the design of the Works, other than the Selected Agency's design.

## **12.11 Selected Agency's Risks**

All risks of loss of or damage to physical property and of personal injury and death which arise during and in consequence of the performance of the Contract other than the excepted risks, are the responsibility of the Selected Agency.

**12.12 Management Meetings**

MCGM may require the Selected Agency to attend a management meeting. The business of a management meeting shall be to review the plans for progress of the Works.

MCGM shall record the business of management meetings and provide copies of the record to those attending the meeting. The responsibility of the parties for actions to be taken shall be decided by MCGM either at the management meeting or after the management meeting and stated in writing to all those who attended the meeting.

**12.13 Tests**

The Selected Agency will have to perform the mandatory tests as prescribed in the specifications. The Selected Agency shall be solely responsible for:

- a. Carrying out the mandatory tests prescribed in the Specifications, and
- b. For the correctness of the test results, whether preformed.

If MCGM instructs the Selected Agency to carry out a test not specified in the Specification/ Quality Assurance Handbook to check whether any work has a Defect and the test shows that it does, the Selected Agency shall pay for the test and any samples. If there is no defect, the test shall be a compensation event.

The cost of testing shall be borne by the Selected Agency even if the result of the sample confirms or do not confirm to the relevant specifications.

All expenditure required to be incurred in testing shall be borne by the Selected Agency himself.

**12.14 Variations**

MCGM shall, having regard to the scope of the Works and the sanctioned estimated cost, have power to order, in writing, Variations within the scope of the Works he considers necessary or advisable during the progress of the Contract. Such Variations shall form part of the Contract and the Selected Agency shall carry them out and include them in updated Programmes produced by the Selected Agency. Oral orders of MCGM for Variations, unless followed by written confirmation, shall not be taken into account.

**12.15 Payment for Variations**

If rates for Variation items are specified in the Bill of Quantities, the Selected Agency shall carry out such work at the same rate.

**12.16 Operation and Maintenance Manuals**

If Drawings and/or operating and maintenance manuals are required, the Selected Agency shall supply them by the dates stated in the Contract Data.

If the Selected Agency does not supply the Drawings and/or manuals by the dates stated in the contract Data, or they do not receive the MCGM's approval, MCGM shall withhold the amount stated in the Contract Data from payments due to the Selected Agency.

**12.17 Compliance with Labour Regulations**

During continuance of the Contract, the Selected Agency and his sub-Contractors shall abide at all times by all existing labour enactments and rules made there under, regulations, notifications and bye laws of the State or Central Government or local authority and any other labour law (including rules), regulations, bye laws that may be passed or notification that may be issued under any labour law in future either by the State or the Central Government or the local authority.

Furthermore, the Selected Agency shall keep MCGM indemnified in case any action is taken against the MCGM by the competent authority on account of contravention of any of the provisions of any Act or rules made there under, regulations or notifications including amendments. If MCGM is caused to pay or reimburse, such amounts as may be necessary to cause or observe, or for non-observance of the provisions stipulated in the notifications/bye laws/Acts/Rules/regulations including amendments, if any, on the part of the Selected Agency, MCGM shall have the right to deduct any money due to the Selected Agency including his amount of performance guarantee. The MCGM shall also have right to recover from the Selected Agency any sum required or estimated to be required for making good the loss or damage suffered by MCGM.

The Selected Agency shall require his employees to obey all applicable laws, including those concerning safety at work.

The employees of the Selected Agency and the Sub-Contractor in no case shall be treated as the employees of the MCGM at any point of time.

### **12.18 Clarification**

Bidder requiring any clarification on the tender may notify “the MCGM Authority” in writing or by fax or e-mail. They should send in their queries before the date specified in the Bid Data Sheet. “The MCGM Authority” shall Endeavour to respond to the queries within the period specified therein. The responses will be sent by fax and/or e-mail. The MCGM Authority will forward all the queries and its responses thereto, to all purchasers of the TENDER without identifying the source of queries.

“The MCGM Authority” shall Endeavour to respond to the questions raised or clarifications sought by the Bidders. However, the MCGM Authority reserves the right not to respond to any question or provide any clarification, in its sole discretion, and nothing in this Clause shall be taken or read as compelling or requiring the MCGM Authority to respond to any question or to provide any clarification, but not later than the date provided in header data.

“The MCGM Authority” may also on its own motion, if deemed necessary, issue interpretations and clarifications to all Bidders. All clarifications and interpretations issued by the MCGM Authority shall be deemed to be part of the tender. Verbal clarifications and information given by MCGM Authority or its employees or representatives shall not in any way or manner be binding on the MCGM Authority.

### **12.19 Format & Signing of Application**

The Bidder shall provide all the information sought under this TENDER. The MCGM Authority will evaluate only those application that are received in the required formats and complete in all respects. Incomplete and /or conditional Bids shall be liable to rejection.

The Bidder will upload application in One Folder in electronic form which shall contain the scanned certified copies of the documents given below and the documents uploaded has to be digitally signed by the bidder. These copies shall be certified by Practicing Notary approved by the Govt. of Maharashtra or Govt. of India with his stamp, clearly stating his name & registration number, except where original documents are demanded.

**12.20 Marking of Application**

The Bidder shall submit the application in the format specified in the Bid Document, together with the documents, upload in folder as “Bidder” together with their respective enclosures

Applications submitted by fax, telex, telegram shall not be entertained and shall be rejected outright.

**12.21 Clarification of Financial Bids**

To assist in the examination, evaluation and comparison of Bids, MCGM may, at his discretion, ask any bidder for clarification of his Bid, including breakdown of unit rates. The request for clarification and the response shall be in writing or by post/facsimile/e-mail. No Bidder shall contact MCGM officials on any matter relating to his bid from the time of the bid opening to the time the contract is awarded. Any effort by the Bidder to influence the MCGM officials in the bid evaluation, bid comparison or contract award decisions may result in the rejection of the Bidder's bid.

**12.22 Official Secrecy**

The Selected Agency shall of all the persons employed in any works in connection with the contract that the India Official Secrets Act 1923 (XIX of 1923) applies to them and will continue to apply even after execution of the said works and they will not disclose any information regarding this contract to any third party. The Selected Agency shall also bring into notice that, any information found to be leaked out or disclosed the concern person as well as the Selected Agency will be liable for penal action; further the Corporation will be at liberty to terminate the contract without notice.

**12.23 Subsequent Legislation**

If on the day of submission of bids for the contract, there occur changes to any National or State statute, Ordinance, decree or other law or any regulation or By-laws or any local or other duly constituted authority or the introduction of any such National or State Statute, Ordinance, decree or by which causes additional or reduced cost to the Selected Agency, such additional or reduced cost shall, after due consultation with the Selected Agency, be determined by the concerned authority of MCGM and shall be added to or deducted from

the Contract Price with prior approval of competent authority and MCGM shall notify the Selected Agency accordingly .MCGM reserve the right to take decision in respect of addition/reduction of cost in contract.

#### **12.24 Patent, Rights & Royalties**

The Selected Agency shall save harmless and indemnify the Corporation from and against all claims and proceedings for or on account of infringement of any Patent rights, design trademark or name of other protected rights in respect of any constructional plant, machine work, or material used for or in connection with the Works or any of them and from and against all claims, proceedings, damages, costs, charges and expenses whatsoever in respect thereof or in relation thereto. Except where otherwise specified, the Selected Agency shall pay all tonnage and other royalties, rent and other payments or compensation, if any, required for the works.

#### **12.25 Payment, Taxes & Claims**

➤ **The limit for unforeseen Risks**

Under no circumstances whatever the Selected Agency shall be entitled to any compensation from MCGM on any account unless the Selected Agency shall have submitted a claim in writing to MCGM within 1 month of the case of such claim occurring.

➤ **No interest for delayed payments due to disputes, etc.**

It is agreed that the Municipal Corporation of Greater Mumbai or its representative or Officer shall not be liable to pay any interest or damage with respect of any moneys or balance which may be in its or its representative's or officer's hands owing to any dispute or difference or claim or misunderstanding between the Municipal Corporation of Greater Bombay or its representative or Officer on the one hand and the Selected Agency on the other, or with respect to any delay on the part of the Municipal Corporation of Greater Bombay or representative or Officers in making periodical or final payments or in any other respect whatever.

#### **12.26 Receipts to be signed in firm's name by any one of the partners**

Every receipt for money which may become payable or for any security which may become transferable to the Selected Agency under these present shall, if signed in the partnership name by any one of the partners, be a good and sufficient discharge to the Commissioner

and Municipal Corporation in respect of the money or security purporting to be acknowledged thereby, and in the event of death of any of the partners during the pendency of this contract, it is hereby expressly agreed that every receipt by any one of the surviving partners shall, if so signed as aforesaid, be good and sufficient discharge as aforesaid provided that nothing in this clause contained shall be deemed to prejudice or effect any claim which the Commissioner or the Corporation may hereafter have against the legal representatives of any partners so dying or in respect of any breach of any of the conditions thereof, provided also that nothing in this clause contained shall be deemed prejudicial or affect the respective rights or obligations of the Selected Agency and of the legal representatives of any deceased Selected Agency interest.

#### **12.27 Proprietary data**

All documents and other information supplied by the Authority or submitted by a Selected Agency to MCGM Authority shall remain or become the property of MCGM Authority. Selected Agency are to treat all information as strictly confidential and shall not use it for any purpose other than for preparation and submission of their Application. MCGM Authority will not return any Application or any information provided along therewith.

#### **12.28 Correspondence with the Selected Agency**

Save and except as provided in this TENDER, MCGM Authority shall not entertain any correspondence with any Selected Agency in relation to the acceptance or rejection of any Application.

#### **12.29 Taxes**

G.S.T. and other state levies/ cess which are not subsumed under GST will be applicable. The tenderer shall quote inclusive of all taxes. It is clearly understood that MCGM will not bear any additional liability towards payment of any Taxes & Duties.

Wherever the services to be provided by the Tenderers falls under Reverse Charge Mechanism, the price quoted shall be exclusive of GST, but inclusive of Taxes/ Duties/ Cess other than GST, if any.

Rates accepted by MCGM shall hold good till completion of work and no additional individual claim shall be admissible on account of fluctuations in market rates, increase in

taxes/ any other levies/ tolls etc. Except that payment/ recovery for overall market situation shall be made as per price variation.

### **12.30 Contract Execution**

All required documents for execution of the contract shall be submitted within 30 days from the date of issue of letter of acceptance. If the documents are not submitted within the stipulated time a penalty of Rs 5000/- per day will be applicable to the Bidder. All contract documents need to be duly affixed with stamp duty properly signed along with evidence/proof of payment of security/contract deposit/ within 30 days from the date of letter of acceptance received by him.

If the amount of the Contract Deposit to be paid above is not paid within 30 days from the date of issue of Letter of Acceptance, the Tender / Contractor already accepted shall be considered as cancelled and legal steps be taken against the Bidder for recovery of the amounts.

The amount of Bank Guarantee (BG) retained by the MCGM shall be released after expiry of period up to which the contractor has agreed to maintain the work in good order is over. In the event of the contractor failing or neglecting to complete the rectification work within the period up to which the contractor has agreed to maintain the work in good order, the amount of Bank Guarantee (BG) retained by MCGM shall be adjusted to- wards the excess cost incurred by the Department on rectification work.

### **12.31 Bribery and Insolvency**

Contract may be rescinded and Bank Guarantee (BG) forfeited for bribing a public officer or if contractor becomes insolvent.

If the contractor assigns or sublets his contracts or attempt so to do, or become insolvent or commence any proceeding to get himself adjudicated and insolvent or make any composition with his creditors, or attempt so to do or if bribe, gratuity, gift, loan, perquisite, reward or advantage, pecuniary or otherwise, shall either directly or indirectly be given promised or offered by the contractor or any of his servants or agents through any public officer, or person in the employ of MCGM/Govt. in any way relating to his office or employment, or if any such officer or person shall become in any way directly or indirectly interested in the contract the Engineer In-charge may thereupon, by notice in writing



rescind the contract and the Bank Guarantee (BG) of the Contractor shall thereupon stand forfeited and be absolutely at the disposal of MCGM and the same consequences shall ensure as if the contract had been rescinded under above clause J hereof; and in addition the contractor shall not be entitled to recover or be paid for any work therefore actually performed under the contract.

### **12.32 Fees**

Total fees to be paid to the Selected Agency for the execution of this Contract shall as per the Section 9 of Commercial Bid Formats

**<<NOTE >>: While Preparing the Contract please copy paste the pertinent section from Section 9 Commercial Bid Format.**

The fees shall be inclusive of GST, Income Tax, duties, fees, levies, charges, and commissions as applicable under the relevant laws of India. Should there be a change in applicable taxes, the actual taxes on the date of billing would prevail.

### **12.33 Use and Acquisition of Assets during the term**

The Selected Agency shall–

1. Take all reasonable and proper care of the entire hardware and software, network or any other information technology infrastructure components used for the project and other facilities leased/owned by the Selected Agency exclusively in terms of the delivery of the services as per this CA (hereinafter the “Assets”) in proportion to their use and control of such Assets which will include all upgrades/enhancements and improvements to meet the needs of the project arising from time to time
2. Term “Assets” also refers to all the hardware / Software / furniture / data / documentations / manuals / catalogues / brochures / or any other material procured, created or utilized by the Selected Agency.
3. Keep all the tangible Assets in good and serviceable condition (reasonable wear and tear excepted) suitably upgraded subject to the relevant standards as stated in the bid to meet the SLAs mentioned in the contract and during the entire term of the Agreement
4. Ensure that any instructions or manuals supplied by the manufacturer of the Assets

- for use of Assets and which are provided to the Selected Agency will be followed by the Selected Agency and any person who will be responsible for the use of the Asset
5. Take such steps as may be recommended by the manufacturer of the Assets and notified to the Selected Agency or as may be necessary to use the Assets in a safe manner
  6. To the extent that the Assets are under the control of the Selected Agency, keep the Assets suitably housed and in conformity with any statutory requirements from time to time applicable to them
  7. Not, knowingly or negligently use or permit any of the Assets to be used in contravention of any statutory provisions or regulation or in any way contrary to law
  8. Use the Assets exclusively for the purpose of providing the Services as defined in the contract
  9. Ensure the integration of the software with hardware to be setup and the current Assets in order to ensure the smooth operations of the entire solution architecture to provide efficient services to MCGM of this Project in an efficient and speedy manner
  10. Selected Agency shall not use MCGM data to provide services for the benefit of any third party, as a service bureau or in any other manner

#### **12.34 Security and safety**

1. The Selected Agency will comply with the directions issued from time to time by MCGM and the standards related to the security and safety in so far as it applies to the provision of the Services
2. Adherence to basic eGovernance Guidelines and Standards for data structure (if any) shall be adhered to.
3. Selected Agency shall also comply with MCGM / Government of Maharashtra's / Government of India's information technology security and standard policies in force from time to time as applicable. If required, MCGM shall share the relevant guidelines and standards to the Selected Agency from time to time.
4. Selected Agency shall use reasonable endeavours to report forthwith in writing to all the partners / contractors about the civil and criminal liabilities accruing due to any unauthorized access (including unauthorized persons who are employees of any Party) or interference with MCGM's data, facilities or Confidential Information.
5. The Selected Agency shall upon reasonable request by MCGM or his/her nominee(s)

participate in regular meetings when safety and information technology security matters are reviewed.

6. Selected Agency shall promptly report in writing to MCGM any act or omission which they are aware that could have an adverse effect on the proper conduct of safety and information technology security at MCGM.

### **12.35 Indemnity**

The Selected Agency agrees to indemnify and hold harmless MCGM, its officers, employees and agents(each an “Indemnified Party”) promptly upon demand at any time and from time to time, from and against any and all losses , claims, damages, liabilities, costs (including reasonable attorney’s fees and disbursements) and expenses (collectively, “Losses”) to which the Indemnified Party may become subject, in so far as such losses directly arise out of, in any way relate to, or result from

- i. Any mis-statement or any breach of any representation or warranty made by the Selected Agency or
- ii. The failure by the Selected Agency to fulfil any covenant or condition contained in this Agreement, including without limitation the breach of any terms and conditions of this Agreement by any employee or agent of the Selected Agency. Against all losses or damages arising from claims by third Parties that any Deliverable (or the access, use or other rights thereto), created by Selected Agency pursuant to this Agreement, or any equipment, software, information, methods of operation or other intellectual property created by Selected Agency or sub-contractors pursuant to this Agreement, or the SLAs (I) infringes a copyright, trade mark, trade design enforceable in India, (II) infringes a patent issued in India, or (III) constitutes misappropriation or unlawful disclosure or use of another Party’s trade secretes under the laws of India (collectively, “Infringement Claims”); provided, however, that this will not apply to any Deliverable (or the access, use or other rights thereto) created by (A) <insert name of the Project> by itself or through other persons other than Selected Agency or its sub-contractors; (B) Third Parties (i.e., other than Selected Agency or sub-contractors) at the direction of MCGM, or

- iii. Any compensation / claim or proceeding by any third party against MCGM arising out of any act, deed or omission by the Selected Agency or
- iv. Claim filed by a workman or employee engaged by the Selected Agency for carrying out work related to this Agreement. For the avoidance of doubt, indemnification of Losses pursuant to this section shall be made in an amount or amounts sufficient to restore each of the Indemnified Party to the financial position it would have been in had the losses not occurred.

Any payment made under this Agreement to an indemnity or claim for breach of any provision of this Agreement shall include applicable taxes.

### **12.36 Third Party Claims**

- a. Subject to Sub-clause (b) below, the Selected Agency(the “Indemnifying Party”) indemnifies MCGM (Indemnified Party) from and against all losses, claims litigation and damages on account of bodily injury, death or damage to tangible personal property arising in favour or any person, corporation or other entity (including the Indemnified Party) attributable to the Indemnifying Party’s performance or non-performance under this Agreement or the SLAs.
- b. The indemnities set out in Sub-clause (a) above shall be subject to the following conditions:
  - i. The Indemnified Party, as promptly as practicable, informs the Indemnifying Party in writing of the claim or proceedings and provides all relevant evidence, documentary or otherwise;
  - ii. The Indemnified Party shall, at the cost and expenses of the Indemnifying Party, give the Indemnifying Party all reasonable assistance in the defence of such claim including reasonable access to all relevant information, documentation and personnel. The indemnifying party shall bear cost and expenses and fees of the Attorney on behalf of the Indemnified Party in the litigation, claim.
  - iii. If the Indemnifying Party does not assume full control over the defence of a claim as provided in this Article, the Indemnifying Party may participate in such defence at its sole cost and expense, and the Indemnified Party will have the right to defend the claim in such manner as it may deem appropriate,

and the cost and expense of the Indemnified Party will be borne and paid by the Indemnifying Party.

- iv. The Indemnified Party shall not prejudice, pay or accept any proceedings or claim, or compromise any proceedings or claim, without the written consent of the Indemnifying Party;
- v. Selected Agency hereby indemnify and hold indemnified MCGM harmless from and against any and all damages, losses, liabilities, expenses including legal fees and cost of litigation in connection with any action, claim, suit, proceedings as if result of claim made by the third party directly or indirectly arising out of or in connection with this agreement.
- vi. All settlements of claims subject to indemnification under this Article will:  
(a) be entered into only with the consent of the Indemnified Party, which consent will not be unreasonably withheld and include an unconditional release to the Indemnified Party from the claimant for all liability in respect of such claim; and (b) include any appropriate confidentiality agreement prohibiting disclosure of the terms of such settlement;
- vii. The Indemnified Party shall take steps that the Indemnifying Party may reasonably require to mitigate or reduce its loss as a result of such a claim or proceedings; and
- viii. In the event that the Indemnifying Party is obligated to indemnify an Indemnified Party pursuant to this Article, the Indemnifying Party will, upon payment of such indemnity in full, be subrogated to all rights and defences of the Indemnified Party with respect to the claims to which such indemnification relates;
- ix. In the event that the Indemnifying Party is obligated to indemnify the Indemnified Party pursuant to this Article, the Indemnified Party will be entitled to invoke the Bank Guarantee, if such indemnity is not paid, either in full or in part, and on the invocation of the Bank Guarantee, the Indemnifying Party shall be subrogated to all rights and defences of the Indemnified Party with respect to the claims to which such indemnification relates.

Selected Agency will defend or settle third party claims against MCGM solely attributable to the Selected Agency's infringement of any copyrights, trademarks or industrial design rights alleged to have occurred in respect of Selected Agency branded

hardware/software/deliverables etc. (together “deliverables”) supplied by the Selected Agency. The Selected Agency shall pay all costs, damages and attorney's fees that a court finally awards.

MCGM shall provide the Selected Agency with prompt notice of such claim and extend full cooperation and assistance, information and authority reasonably necessary to defend or settle such claim. The Selected Agency will have adequate opportunity to control the response thereto and the defence thereof.

Further as an exclusion, the Selected Agency shall have no obligation for any claim of infringement to the extent arising from use of the deliverables in a way not indicated in the statement of work or in any specifications or documentation provided with such deliverable.

### **12.37 Publicity**

Any publicity by the Selected Agency in which the name of MCGM is to be used should be done with the explicit written permission of The Municipal Commissioner, IT, Municipal Corporation of Greater Mumbai.

### **12.38 Warranties**

- a. The Selected Agency warrants and represents to MCGM that:
  - i. It has full capacity and authority and all necessary approvals to enter into and to perform its obligations under this Agreement;
  - ii. This Agreement is executed by a duly authorized representative of the Selected Agency;
  - iii. It shall discharge its obligations under this Agreement with due skill, care and diligence so as to comply with the service level agreement.
- b. In the case of the SLAs, the Selected Agency warrants and represents to MCGM, that:
  - i. The Selected Agency has full capacity and authority and all necessary approvals to enter into and perform its obligations under the SLAs and to provide the Services;
  - ii. The SLAs shall be executed by a duly authorized representative of the Selected Agency;
  - iii. The Services will be provided and rendered by appropriately qualified, trained and experienced personnel as mentioned in the bid;

- iv. Selected Agency has and will have all necessary licenses, approvals, consents of third Parties free from any encumbrances and all necessary technology, hardware and software to enable it to provide the Services;
- v. The Services will be supplied in conformance with all laws, enactments, orders and regulations applicable from time to time;
- vi. Selected Agency will warrant that the solution provided under the contract is new, of the most recent higher version /models and incorporate all recent improvements in design and materials unless provided otherwise in the contract.
- vii. The Selected Agency shall ensure defect free operation of the entire solution and shall replace any such components, equipment, software and hardware which are found defective and during the entire contract period the Selected Agency shall apply all the latest upgrades/patches/releases for the software after appropriate testing. No additional costs shall be paid separately for the warranty other than what are the costs quoted by the Selected Agency and as specified in the contract.
- viii. If the Selected Agency uses in the course of the provision of the Services, components, equipment, software and hardware manufactured by any third party and which are embedded in the Deliverables or are essential for the successful use of the Deliverables, it will pass-through third-party manufacturer's Warranties relating to those components, equipment, software and hardware to the extent possible.

The Selected Agency will repair/correct the warranty defect in the Selected Agency branded hardware/software or correct a material non-conformance to specifications in accordance with the terms and conditions mutually agreed between the parties during the agreed warranty period and in accordance with the terms of the respective OEMs/Software vendors. Further, Selected Agency will not be responsible for any breach of warranty or support resulting from unauthorized changes made to the software/hardware supplied by it.

Notwithstanding what has been stated elsewhere in this Agreement and the Schedules attached herein, in the event the Selected Agency is unable to meet the obligations pursuant to the Implementation of the project, Operations and Maintenance Services and any related scope of work as stated in this Agreement and the Schedules attached herein, MCGM will have the option to invoke the Bank Guarantee after serving a written notice of thirty (30) days to the Selected Agency.

**12.39 Force Majeure**

The Selected Agency shall not be liable for forfeiture of its Bank Guarantee, imposition of liquidated damages or termination for default, if and to the extent that its delay in performance or other failure to perform its obligations under the contract is the result of an event of Force Majeure. For purposes of this Clause, “Force Majeure” means an event beyond the “reasonable” control of the Selected Agency, not involving the Selected Agency’s fault or negligence and not foreseeable. Unforeseen circumstances or causes beyond the control of the Selected Agency include but are not limited to acts of God, war, riot, acts of civil or military authorities, fire, floods, accidents, terrorist activity, strikes or shortages of transportation facilities, fuel, energy, labour or material.

For the Selected Agency to take benefit of this clause it is a condition precedent that the Selected Agency must promptly notify MCGM, in writing of such conditions and the cause thereof within five calendar days of the arising of the Force Majeure event. MCGM, or the consultant / committee appointed by MCGM shall study the submission of the Selected Agency and inform whether the situation can be qualified one of Force Majeure. Unless otherwise directed by MCGM in writing, the Selected Agency shall continue to perform its obligations under the resultant Agreement as far as it is reasonably practical and shall seek all reasonable alternative means for performance of services not prevented by the existence of a Force Majeure event.

In the event of delay in performance attributable to the presence of a force majeure event, the time for performance shall be extended by a period(s) equivalent to the duration of such delay. If the duration of delay continues beyond a period of 30 days, MCGM and the Selected Agency shall hold consultations with each other in an endeavour to find a solution to the problem.

Notwithstanding anything to the contrary mentioned above, the decision of MCGM shall be final and binding on the Selected Agency.

**12.40 Resolution of Disputes**

This Contract shall be governed by laws of India. Disputes arising out of this Agreement shall be first referred to the senior executives of each party for an amicable solution. If the dispute is not resolved within a period of thirty (30) days, the same shall be referred to



arbitration in accordance with Arbitration and Conciliation Act, 1996 (including all amendments thereto).

Each party shall appoint one arbitrator each and the two appointed arbitrators shall appoint the third arbitrator. The decision of the arbitrators shall be final and binding on both parties. The venue of arbitration shall be Mumbai, India. Subject to the above, this Agreement shall be subject to the jurisdiction of the courts of Mumbai, India.

#### **12.41 Risk Purchase Clause**

In the event Selected Agency fails to execute the project as stipulated in the CA, or as per the directions given by MCGM from time to time, MCGM reserves the right to procure similar services from the next eligible Bidder or from alternate sources at the risk and cost of the Selected Agency. Before taking such a decision, MCGM shall serve a notice period of one month to the Selected Agency.

The 30-day notice period shall be considered as the 'Cure Period' to facilitate the Selected Agency to cure the breach. The provision for Risk Purchase shall be evoked in the event the Selected Agency fails to correct the breach within the 'Cure Period'.

The Selected Agency's liability under the resultant Agreement shall be determined as per the Law in force for the time being. The Selected Agency shall be liable to MCGM for loss or damage occurred or caused or likely to occur on account of any act of omission on the part of the Selected Agency and its employees, including loss caused to MCGM on account of defect in goods or deficiency in services on the part of Selected Agency or his agents or any person / persons claiming through or under said Selected Agency.

Selected Agency's aggregate liability in connection with obligations undertaken as a part of this contract regardless of the form or nature of the action giving rise to such liability, shall be at actual and limited to the amount paid by MCGM for:

- (i) The particular hardware/software; or
- (ii) Services provided during the twelve (12) months immediately preceding the date of the claim;

that in each case is the subject of the claim.

This limit shall not apply to damages for bodily injury (including death) and damage to real property and tangible personal property for which the Selected Agency is legally liable.

**12.42 Conflict of Interest**

The Selected Agency shall disclose to MCGM in writing, all actual and potential conflicts of interest that exist, arise or may arise (either for the Selected Agency or its team) in the course of performing the Services as soon as it becomes aware of such a conflict. Selected Agency shall hold MCGM's interest paramount, without any consideration for future work, and strictly avoid conflict of interest with other assignments.

**12.43 Data Ownership**

All the data created as the part of the project shall be owned by MCGM. The Selected Agency shall take utmost care in maintaining security, confidentiality and backup of this data. Access to the data / systems shall be given by the Selected Agency only to the personnel working on the projects and their names and contact details shall be shared with MCGM in advance. MCGM / its authorized representative(s) shall conduct periodic / surprise security reviews and audits, to ensure the compliance by the Selected Agency to data / system security.

The ownership of the application and the data shall rest with MCGM.

**12.44 Fraud and Corruption**

MCGM requires that Selected Agency must observe the highest standards of ethics during the execution of the contract. In pursuance of this policy, MCGM defines, for the purpose of this provision, the terms set forth as follows:

- a. "Corrupt practice" means the offering, giving, receiving or soliciting of anything of value to influence the action of MCGM in contract executions.
- b. "Fraudulent practice" means a misrepresentation of facts, in order to influence a procurement process or the execution of a contract, to MCGM, and includes collusive practice among bidders (prior to or after bid submission) designed to establish bid prices at artificially high or non-competitive levels and to deprive MCGM of the benefits of free and open competition.
- c. "Undesirable practice" means (i) establishing contact with any person connected with or employed or engaged by MCGM with the objective of canvassing, lobbying or in any manner influencing or attempting to influence the Selection Process; or (ii) having a Conflict of Interest; and

- d. “Restrictive practice” means forming a cartel or arriving at any understanding or arrangement among Bidders with the objective of restricting or manipulating a full and fair competition in the Selection Process.
- e. “Coercive Practices” means harming or threatening to harm, directly or indirectly, persons or their property to influence their participation in the execution of contract.

If it is noticed that the Selected Agency has indulged into the Corrupt / Fraudulent / Undesirable / Coercive practices, it will be a sufficient ground for MCGM for termination of the contract and initiate black-listing of the vendor.

#### **12.45 Exit Management**

##### **i. Exit Management Purpose**

This clause sets out the provisions, which will apply during Exit Management period. The Parties shall ensure that their respective associated entities carry out their respective obligations set out in this Exit Management Clause.

##### **ii. Confidential Information, Security and Data**

Selected Agency will promptly, on the commencement of the exit management period, supply to MCGM or its nominated agencies the following:

- a. Information relating to the current services rendered and performance data relating to the performance of the services; documentation relating to the project; any other data and confidential information created as part of or is related to this project;
- b. Project data as is reasonably required for purposes of the project or for transitioning of the services to its replacing successful Bidder in a readily available format.
- c. All other information (including but not limited to documents, records and agreements) relating to the services reasonably necessary to enable MCGM and its nominated agencies, or its replacing vendor to carry out due diligence in order to transition the provision of the Services to MCGM or its nominated agencies, or its replacing vendor (as the case may be).
- d. The Selected Agency shall retain all of the above information with them for 30 days after the termination of the contract, post which the provider has to wipe/purge/delete all information created or retained as part of this project.

- e. Selected Agency will sign a Non-Disclosure Agreement with MCGM IT Department.  
The format for the same has been included in Annexure section of this bid document.

**iii. Rights of Access to Information**

At any time during the exit management period, the Selected Agency will be obliged to provide an access of information to MCGM and / or any Replacing Vendor in order to make an inventory of the Assets (including hardware / Software / Active / passive), documentations, manuals, catalogues, archive data, Live data, policy documents or any other material related to implementation of the application for MCGM.

**iv. Exit Management Plan**

Successful Bidder shall provide MCGM with a recommended “Exit Management Plan” within 90 days of signing of the contract, which shall deal with at least the following aspects of exit management in relation to the SLA as a whole and in relation to the Project Implementation, the Operation and Management SLA and Scope of work definition.

- a. A detailed program of the transfer process that could be used in conjunction with a Replacement Vendor including details of the means to be used to ensure continuing provision of the services throughout the transfer process or until the cessation of the services and of the management structure to be used during the transfer;
- b. Plans for the communication with such of the Successful Bidder, staff, suppliers, customers and any related third party as are necessary to avoid any material detrimental impact on Project’s operations as a result of undertaking the transfer;
- c. Plans for provision of contingent support to the implementation of hosted Project and Replacement Vendor for a reasonable period (minimum one month) after transfer.
- d. Exit Management Plan shall be presented by the Selected Agency to and approved by MCGM or its nominated agencies.
- e. The terms of payment as stated in the Terms of Payment Schedule include the costs of the Selected Agency complying with its obligations under this Schedule.
- f. During the exit management period, the Selected Agency shall use its best efforts to deliver the services.

- g. Payments during the Exit Management period shall be made in accordance with the Terms of Payment Schedule.

#### **12.46 Termination of contract**

MCGM may, without prejudice to any other remedy under this Contract and applicable law, reserves the right to terminate for breach of contract by providing a written notice of 30 days stating the reason for default to the Selected Agency and terminate the contract either in whole or in part:

- If the Selected Agency fails to deliver any or all of the project requirements / operationalization / Operational Acceptance of project within the time frame specified in the contract; or
- If the Selected Agency fails to perform any other obligation(s) under the contract.

Prior to providing a notice of termination to the Selected Agency, MCGM shall provide the Selected Agency with a written notice of 30 days instructing the Selected Agency to cure any breach/ default of the Contract, if MCGM is of the view that the breach may be rectified.

On failure of the Selected Agency to rectify such breach within 30 days, MCGM may terminate the contract by providing a written notice of 30 days to the Selected Agency, provided that such termination will not prejudice or affect any right of action or remedy which has accrued or will accrue thereafter to MCGM. In such an event the Selected Agency shall be liable for penalty imposed by MCGM.

In the event of termination of this contract for any reason whatsoever, MCGM is entitled to impose any such obligations and conditions and issue any clarifications as may be necessary to ensure an efficient transition and effective continuity of the services which the Selected Agency shall be obliged to comply with and take all available steps to minimize the loss resulting from that termination/ breach, and further allow and provide all such assistance to MCGM and/ or succeeding vendor, as may be required, to take over the obligations of the Selected Agency in relation to the execution/ continued execution of the requirements of this contract.

**12.47 Termination for Convenience**

- a) MCGM, by notice sent to Selected Agency, may terminate the Contract, in whole or in part, at any time for its convenience. The notice of termination shall specify that termination is for MCGM's convenience, the extent to which performance of the Selected Agency under the Contract is terminated, and the date upon which such termination becomes effective.
- b) The deliverables/ Services that are complete and ready for delivery within twenty-eight (28) days after the Selected Agency's receipt of notice of termination shall be accepted by MCGM at the Contract terms and prices. For the remaining deliverables/ services, MCGM may elect:
  - I. to have any portion completed and delivered at the Contract terms and prices; and/or
  - II. to cancel the remainder and pay to the Selected Agency an agreed amount for partially completed deliverables and Related Services.

**12.48 Miscellaneous****a. Confidentiality**

“Confidential Information” means all information including Project Data (whether in written, oral, electronic or other format) which relates to the technical, financial and operational affairs, business rules, citizen information, design rights, know-how and personnel of each Party and its affiliates which is disclosed to or otherwise learned by the other Party or its partners (whether a Party to the contract or to the SLA) in the course of or in connection with the contract (including without limitation such information received during negotiations, location visits and meetings in connection with the contract or to the SLA) or pursuant to the contract to be signed subsequently.

Except with the prior written permission of MCGM, the Selected Agency (including all partners) and its Personnel shall not disclose such confidential information to any person or entity not expected to know such information by default of being associated with the project, nor shall the Selected Agency and its Personnel make public the recommendations formulated in the course of, or as a result of the project. In matters

pertaining to privacy of data, the Selected Agency (including all partners) shall not use any data for analytical/commercial reasons whatsoever.

The Selected Agency recognizes that during the term of this Agreement, sensitive data will be procured and made available to it, its partners and agents and others working for or under the Selected Agency. Disclosure or usage of the data by any such recipient may constitute a breach of law applicable causing harm not only to the Department whose data is used but also to its stakeholders. The function of MCGM requires the Selected Agency, its partners and agents to demonstrate utmost care, sensitivity and strict confidentiality. Any breach of this Article will result in MCGM its nominees receiving a right to seek injunctive relief and damages, from the Selected Agency.

The restrictions of this Article shall not apply to confidential information that:

- i. Is or becomes generally available to the public through no breach of this Article by the Recipient; and
- ii. Was in the recipient's possession free of any obligation of confidence prior to the time of receipt of it by the Recipient hereunder; and
- iii. Is developed by the Recipient independently of any of discloser's Confidential Information; and
- iv. Is rightfully obtained by the Recipient from third Parties authorized at that time to make such disclosure without restriction; and
- v. Is identified in writing by the Discloser as no longer proprietary or confidential; or
- vi. Is required to be disclosed by law, regulation or Court Order, provided that the recipient gives prompt written notice to the Discloser of such legal and regulatory requirement to disclose so as to allow the Discloser reasonable opportunity to contest such disclosure.

To the extent that such disclosure is required for the purposes of this Agreement, either Party may disclose Confidential Information to:

- i. Its employees, agents and independent contractors and to any of its affiliates and their respective independent contractors or employees; and
- ii. Its professional advisors and auditors, who require access for the purposes of this Agreement, whom the relevant Party has informed of its obligations under this Article and in respect of whom the relevant Party has informed of its

obligations under this Article has used commercially reasonable efforts to ensure that they are contractually obliged to keep such Confidential Information confidential on terms substantially the same as set forth in this Article. Either Party may also disclose confidential Information or any entity with the other Party's prior written consent.

The provisions of this Article shall survive the expiration or any earlier termination of this Agreement.

**b. Standards of Performance**

The Selected Agency shall provide the services and carry out their obligations under the Contract with due diligence, efficiency and professionalism/ethics in accordance with generally accepted professional standards and practices. The Selected Agency shall always act in respect of any matter relating to this contract. The Selected Agency shall abide by all the applicable provisions/Acts/Rules/ Regulations, Standing orders, etc. of Information Technology as prevalent in the country. The Selected Agency shall also conform to the standards laid down by Government of Maharashtra or Government of India from time to time. Such standards and guidelines shall be shared with the Selected Agency by MCGM up on signing of the Contract.

**c. Care to be taken while working at MCGM Office**

Data for the application should be stored in a Tier 4 data centre empanelled by MEITY and compliant to PII information management standards set by ISO, PCI DSS, SSAE 16, IT policies set by the Govt. of India.

Selected Agency should follow instructions issued by concerned Competent Authority from time to time for carrying out work at designated places. Selected Agency should ensure that there is no damage caused to any private or public property. In case such damage is caused, Selected Agency shall immediately bring it to the notice of concerned organization and MCGM in writing and pay necessary charges towards fixing of the damage.

Selected Agency shall ensure that its employees/representatives don't breach privacy of any citizen or establishment during the course of execution or maintenance of the project.

**d. Compliance with Labour regulations**



The Selected Agency shall pay fair and reasonable wages to the workmen employed, for the contract undertaken and comply with the provisions set forth under the Minimum wages Act and the Contract Labour Act 1970. The salary of the manpower working on MCGM project should be paid using ECS / NEFT / RTGS. A record of the payments made in this regard should be maintained by the Selected Agency. Upon request, this record shall be produced to the appropriate authority in MCGM and/or Judicial Body. If complaints are received by MCGM (or any appropriate authority) appropriate action (Liquidation of Security Deposit, Blacklisting, etc.) may be initiated as deemed necessary against the Selected Agency. The employees of the Selected Agency in no case shall be treated as the employees of the MCGM at any point of time.

**e. Independent Contractor**

Nothing in this Agreement shall be construed as establishing or implying any partnership or joint venture or employment relationship between the Parties to this Agreement. Except as expressly stated in this Agreement nothing in this Agreement shall be deemed to constitute any Party as the agent of any other Party or authorizes either Party (i) to incur any expenses on behalf of the other Party, (ii) to enter into any engagement or make any representation or warranty on behalf of the other Party, (iii) to pledge the credit of or otherwise bind or oblige the other Party, or (iv) to commit the other Party in any manner whatsoever in each case without obtaining the other Party's prior written consent.

**f. Waiver**

A waiver of any provision or breach of this Agreement must be in writing and signed by an authorized official of the Party executing the same. No such waiver shall be construed to affect or imply a subsequent waiver of the same provision or subsequent breach of this Agreement.

**g. Notices**

Any notice or other document, which may be given by either Party under this Agreement, shall be given in writing in person or by pre-paid recorded delivery post. In relation to a notice given under this Agreement, any such notice or other document shall be addressed to the other Party's principal or registered office address as set out below-

MCGM:

Director, IT  
Municipal Corporation of Greater Mumbai,  
Basement, Municipal Head Office, Extension Building, Fort,

---

Tel: -----

Fax: -----

Selected Agency:

---

Tel: -----

Fax: -----

Any notice or other document shall be deemed to have been given to the other Party when delivered (if delivered in person) between the hours of 9.30 A.M and 5.30 P.M. at the address of the other Party set forth above or on the next working day thereafter if delivered outside such hours, and seven calendar days from the date of posting (if by letter).

**h. Personnel/Employees**

- i. Personnel/employees assigned by Selected Agency to perform the services shall be employees of Selected Agency, and under no circumstances will such personnel be considered as employees of MCGM. Selected Agency shall have the sole responsibility for supervision and control of its personnel and for payment of such personnel's employee's entire compensation, including salary, legal deductions withholding of income taxes and social security taxes, worker's compensation, employee and disability benefits and the like and shall be responsible for all employer obligations under all laws as applicable from time to time. MCGM shall not be responsible for the above issues concerning to personnel of Selected Agency.
- ii. Selected Agency shall use its best efforts to ensure that sufficient Selected Agency personnel are employed to perform the Services, and that, such personnel have appropriate qualifications to perform the Services. MCGM or its nominated agencies shall have the right to require the removal or replacement of any Selected Agency personnel performing work under this Agreement. In the event that

MCGM requests that any Selected Agency personnel be replaced, the substitution of such personnel shall be accomplished pursuant to a mutually agreed upon schedule and upon clearance of the personnel based on profile review and personal interview by MCGM or its nominated agencies as per defined SLAs. The Selected Agency shall depute quality team for the project and as per requirements MCGM shall have the right to ask Selected Agency to change the team.

- iii. Management (Regional Head / VP level officer) of Selected Agency needs to be involved in the project monitoring and should attend the review meeting from time to time.
- iv. The profiles of resources proposed by Selected Agency in the technical bid, which are considered for Technical bid evaluation, shall be construed as 'Key Personnel' and the Selected Agency shall not remove such personnel without the prior written consent of MCGM. For any changes to the proposed resources, Selected Agency shall provide equivalent or more experienced resources in consultation with MCGM. The penalty applicable for replacement of 'Key Personnel' within the first six months of the contract shall be Rs. 25,000 per change in resource. Maximum one replacement is permissible in the first six months.
- v. Except as stated in this clause, nothing in this Agreement will limit the ability of Selected Agency freely to assign or reassign its employees; provided that Selected Agency shall be responsible, at its expense, for transferring all appropriate knowledge from personnel being replaced to their replacements. MCGM shall have the right to review and approve Selected Agency's plan for any such knowledge transfer. Selected Agency shall maintain the same standards for skills and professionalism among replacement personnel as in personnel being replaced.
- vi. Each Party shall be responsible for the performance of all its obligations under this Agreement and shall be liable for the acts and omissions of its employees and agents in connection therewith.

**i. Variations and Further Assurance**

- a. No amendment, variation or other change to this Agreement or the SLAs shall be valid unless made in writing and signed by the duly authorized representatives of the Parties to this Agreement.
- b. Each Party to this Agreement or the SLAs agree to enter into or execute, without limitation, whatever other agreement, document, consent and waiver and to do all

other things which shall or may be reasonably required to complete and deliver the obligations set out in the Agreement or the SLAs.

**j. Survivability and Waiver**

- i. If any provision of this Agreement or the SLAs, or any part thereof, shall be found by any court or administrative body of competent jurisdiction to be illegal, invalid or unenforceable the illegality, invalidity or unenforceability of such provision or part provision shall not affect the other provisions of this Agreement or the SLAs or the remainder of the provisions in question which shall remain in full force and effect. The relevant Parties shall negotiate in good faith in order to agree to substitute for any illegal, invalid or unenforceable provision a valid and enforceable provision which achieves to the greatest extent possible the economic, legal and commercial objectives of the illegal, invalid or unenforceable provision or part provision within seven working days.
- ii. No failure to exercise or enforce and no delay in exercising or enforcing on the part of either Party to this Agreement or the SLAs of any right, remedy or provision of this Agreement or the SLAs shall operate as a waiver of such right, remedy or provision in any future application nor shall any single or partial exercise or enforcement of any right, remedy or provision preclude any other or further exercise or enforcement of any other right, remedy or provision.

**k. Survivability**

The termination or expiry of this Agreement or the SLAs for any reason shall not affect or prejudice any terms of this Agreement, or the rights of the Parties under them which are either expressly or by implication intended to come into effect or continue in effect after such expiry or termination.

**12.49 Applicable Law**

The contract shall be governed by the laws and procedures prescribed by the Laws prevailing and in force in India, within the framework of applicable legislation and enactment made from time to time concerning such commercial dealings/processing. All legal disputes are subject to the jurisdiction of Mumbai courts only.

**12.50 Stamp Duty Payment**

The stamp duty payable for the contract shall be borne by the Selected Agency IN WITNESS whereof the parties hereto have signed this on the day, month and year first herein above written.

IN WITNESS WHEREOF THE PARTIES HERETO HAVE PUT THEIR HANDS AND SEAL THE DAY AND YEAR FIRST HEREINABOVE WRITTEN.

THE COMMON SEAL )  
of the Municipal Corporation of )  
Greater Mumbai was affixed hereto )  
In the presence of )  
1. )  
2. )

Two members of the Standing Committee )  
of the Municipal Corporation of Greater )  
Mumbai who in token thereof have set )  
their respective hands hereto )  
In the presence of )  
1. )  
2. )

SIGNED, SEALED AND DELIVERED )  
By the within named )  
Shri. \_\_\_\_\_ )  
Dy. Municipal Commissioner (IT) )  
for on behalf of the )  
Municipal Corporation of Greater Mumbai )  
In the presence of )

1. )
2. )

SIGNED, SEALED AND DELIVERED )  
By the within named )  
Shri. \_\_\_\_\_ )  
(Authorized Signatory) of )  
<Selected agency name> )  
In the presence of )  
1. )  
2. )

**Attachments to the Agreement:**

- i. Scope of Services for the Selected Agency
- ii. Detail Commercial bid of the Selected Agency accepted by MCGM
- iii. Corrigendum Document published by MCGM subsequent to the bid for this work
- iv. Bid Document of MCGM for this work
- v. LoI issued by MCGM to the successful Bidder
- vi. The successful Bidder's "Technical Bid" and "Commercial Bid" submitted in response to the bid

**13 Annexure VII: Draft Non-Disclosure Agreement**

(To be submitted on a Rs. 100 Stamp Paper)

This Non-Disclosure Agreement (“Non-Disc”) is made and entered into \_\_\_\_\_ day of \_\_\_\_\_ month \_\_\_\_\_ year (effective date) by and between \_\_\_\_\_ (“Department”) and \_\_\_\_\_ (“Company”).

Whereas, Department and Company have entered into an Agreement (“Agreement”)

\_\_\_\_\_ effective \_\_\_\_\_ for \_\_\_\_\_; and

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

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

**1. Definitions.** As used herein:

- a) The term “Confidential Information” shall include, without limitation, all information and materials, furnished by either Party to the other in connection with citizen/users/persons/customers data, products and/or services, including information transmitted in writing, orally, visually, (e.g. video terminal display) or on magnetic or optical media, and including all proprietary information, customer and prospect lists, trade secrets, trade names or proposed trade names, methods and procedures of operation, commercial or marketing plans, licensed document know-how, ideas, concepts, designs, drawings, flow charts, diagrams, quality manuals, checklists, guidelines, processes, formulae, source code materials, specifications, programs, software packages, codes and other intellectual property relating to the disclosing party’s data, computer database, products and/or services. Results of any tests, sample surveys, analytics, data mining exercises or usages etc. carried out by the receiving party in connection with the Department’s information including citizen/users/persons/customers personal or

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

- b) The term, “Department” shall include the officers, employees, agents, consultants, contractors and representatives of Department.
- c) The term, “Company” shall include the directors, officers, employees, agents, consultants, contractors and representatives of Company, including its applicable affiliates and subsidiary companies.

**2. Protection of Confidential Information:** With respect to any Confidential Information disclosed to it or to which it has access, Company affirms that it shall:

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



- f) Not to discuss with any member of public, media, press, any or any other person about the nature of arrangement entered between Department and Company or the nature of services to be provided by the Company to the Department.
3. **Onus.** Company shall have the burden of proving that any disclosure or use inconsistent with the terms and conditions hereof falls within any of the foregoing exceptions.
4. **Exceptions.** These restrictions as enumerated in section 1 of this Agreement shall not apply to any Confidential Information:
- a) Which is independently developed by Company or lawfully received from another source free of restriction and without breach of this Agreement; or
  - b) After it has become generally available to the public without breach of this Agreement by Company; or
  - c) Which at the time of disclosure to Company was known to such party free of restriction and evidenced by documentation in such party's possession; or
  - d) Which Department agrees in writing is free of such restrictions.
  - e) Which is received from a third party not subject to the obligation of confidentiality with respect to such Information;
5. **Remedies.** Company acknowledges that (a) any actual or threatened disclosure or use of the Confidential Information by Company would be a breach of this agreement and may cause immediate and irreparable harm to Department; (b) Company affirms that damages from such disclosure or use by it may be impossible to measure accurately; and (c) injury sustained by Department may be impossible to calculate and remedy fully. Therefore, Company acknowledges that in the event of such a breach, Department shall be entitled to specific performance by Company of Company's obligations contained in this Agreement. In addition, Company shall indemnify Department of the actual and liquidated damages which may be demanded by Department. Moreover, Department shall be entitled to recover all costs (including reasonable attorneys' fees) which it or they may incur in connection with defending its interests and enforcement of legal rights arising due to a breach of this agreement by Company.
6. **Need to Know.** Company shall restrict disclosure of such Confidential Information to its employees and/or consultants with a need to know (and advise such employees of the obligations assumed herein), shall use the Confidential Information only for the purposes

set forth in the Agreement, and shall not disclose such Confidential Information to any affiliates, subsidiaries, associates and/or third party without prior written approval of the disclosing party.

7. **Intellectual Property Rights Protection.** No license to a party, under any trademark, patent, copyright, design right, mask work protection right, or any other intellectual property right is either granted or implied by the conveying of Confidential Information to such party.
8. **No Conflict.** The parties represent and warrant that the performance of its obligations hereunder do not and shall not conflict with any other agreement or obligation of the respective parties to which they are a party or by which the respective parties are bound.
9. **Authority.** The parties represent and warrant that they have all necessary authority and power to enter into this Agreement and perform their obligations hereunder.
10. **Dispute Resolution.** If any difference or dispute arises between the Department and the Company in connection with the validity, interpretation, implementation or alleged breach of any provision of this Agreement, any such dispute shall be referred to the Hon. Municipal Commissioner, MCGM before arbitration.
  - a) The arbitration proceedings shall be conducted in accordance with the (Indian) Arbitration and Conciliation Act, 1996 and amendments thereof.
  - b) The place of arbitration shall be Mumbai.
  - c) The arbitrator's award shall be substantiated in writing and binding on the parties.
  - d) The proceedings of arbitration shall be conducted in English language.
  - e) The arbitration proceedings shall be completed within a period of 180 days from the date of reference of the dispute to arbitration.
11. **Governing Law.** This Agreement shall be interpreted in accordance with and governed by the substantive and procedural laws of India and the parties hereby consent to the exclusive jurisdiction of Courts and/or Forums situated at Mumbai, India only.
12. **Entire Agreement.** This Agreement constitutes the entire understanding and agreement of the parties, and supersedes all previous or contemporaneous agreement or communications, both oral and written, representations and under standings among the parties with respect to the subject matter hereof.

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

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

**For Department**

Name:

Title:

WITNESSES:

1.

2.

**For Company**

Name:

Title:

WITNESSES:

1.

2.

**14 Annexure VIII: Irrevocable Undertaking**

(On ₹500/- stamp paper)

I Shri / Smt. .... aged, ..... years Indian Inhabitant.  
Proprietor/ Partner / Director of M/s. .... resident at do hereby  
give Irrevocable undertaking as under;

1. I say & undertake that as specified in section 171 of CGST Act, 2017, any reduction in rate of tax on supply of goods or services or the benefit of input tax credit shall be mandatorily passed on to MCGM by way of commensurate reduction in prices.
2. I further say and undertake that I understand that in case the same is not passed on and is discovered at any later stage, MCGM shall be at liberty to initiate legal action against me for its recovery including, but not limited to, an appeal to the Screening Committee of the GST Counsel.
3. I say that above said irrevocable undertaking is binding upon me / my partners / company / other Directors of the company and also upon my / our legal heirs, assignee, Executor, administrator etc.
4. If I fail to compliance with the provisions of the GST Act, I shall be liable for penalty / punishment or both as per the provisions of GST Act.

Whatever has been stated here in above is true & correct to my / our own knowledge & belief.

Solemnly affirmed at

DEPONENT

This day of

BEFORE ME

Interpreted Explained and Identified by me.

## **15 Annexure IX: Format for Exception based Report and Security Compliance Certificate**

All the observations identified during the review of applications and IT Infrastructure must be presented in such a way that contains all the following fields:

- o Identification of auditee
- o Date, time and location of the audit
- o Standard followed
- o Comments against each controls tested
- o Summary of audit findings including identification tests, tools used and results of tests performed (like vulnerability assessment, penetration testing, application security audit etc.)
- o Detailed review approach and methodology
- o Tools used and methodology employed
- o Positive security aspect identified
- o List of vulnerability identified
- o Description of vulnerability
- o Risk rating or severity of vulnerability
- o Category of risks: Very High/ High/ Medium/ Low
- o Test cases used for the assessing the vulnerabilities
- o Illustration of the test cases
- o Proof/evidence (Screenshot) of the vulnerabilities identified
- o Mapping of evidences with observations.
- o Analysis of vulnerability and issue of concern
- o Recommendation with detailed implementation steps / screenshots of all steps for corrective action as per industry standard and best practices.

In addition to the list mentioned above, the report must also have the following sections:

- ❖ Executive Summary
- ❖ Scope of Work
- ❖ Audit activities performed
- ❖ Evidences
- ❖ Conclusion

**Format for Security Compliance Certificate**

<b><u>Vendor Site Compliance Certificate</u></b>		
<b>S. No.</b>	<b>Parameters</b>	<b>Comments of the Security Consultant</b>
1	Features of the SSL certificate implemented for the site	
2	Whether the site is PCI – DSS certified. Only applicable for sites capturing card data on their system	
<b>Security review - evidence</b>		
3 a.	Is a policy for regular application security review in place? Please specify the review cycle.	
3 b.	When was the last review done?	
3 c.	Is there evidence to confirm that the findings have since been closed?	
<b>Security review - evidence</b>		
4 a.	Is there a policy for regular vulnerability assessments in place for the operating system, the database servers, the application servers, the web servers? Please specify the review cycle.	
4 b.	When was the last vulnerability assessment done?	
4 c.	Is there evidence to confirm that the findings have since been closed?	
<b>System configuration &amp; access control</b>		
5	Whether the database application servers are behind the firewall?	
6	Whether the firewall access and administration is limited to network security staff?	
7	Whether regular system checks are done to test firewall strengths for identifying potential weak points (Including remote access to systems by email, internet)?	

8	Whether security patches are reviewed and updated regularly for the system?	
9	Whether internal and external network scanned regularly for vulnerabilities?	
10	Confirm that no internet services like SMTP, HTTP, FTP run by default on the system. Please specifically confirm that these services do not run on application and database servers.	
11	Whether all internet and intranet connections are protected?	
12	Whether wireless network is separate from internal network?	
	<b>Application and Data Security measures</b>	
13	Whether care is taken to see that CW/CID numbers are not stored. Applicable only if site captures card details	
14	Whether care is taken to see card expiry dates are not stored	
15	Whether care is taken to see that VBVC/Secure code detail is neither collected nor stored?	
16	Whether care is taken to see that no net banking username and passwords or HPIN is collected/stored?	
17	Whether access control policies are defined for accessing/modification and manipulation of data?	
	<b>Work Procedure</b>	
18	Whether access to sensitive data is permitted on need to know basis	
19	Whether there is evidence to confirm that sufficient logs are maintained for all transactions to help establish a clear audit trail and assist in dispute resolution	



20	Whether there is evidence to confirm that systems are in place to capture and maintain forensic evidence in a manner that maintains control over evidence and prevents tampering with and collection of false evidence?	
----	---	--

Signature of the Security Consultant.....

Seal

**Disclaimer**

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

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

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

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

whether resulting from negligence or otherwise howsoever caused arising from reliance of any Bidder.