Brihanmumbai Municipal Corporation

Information Technology Department

Request for Bids

RFB No: *2024_MCGM_1059546_1*

Provisioning, Installation, Configuration, Testing, Commissioning, Operations & Maintenance of Information System for Enhancement of IT Security of BMC

Brihanmumbai Municipal Corporation
(Information Technology Department)

No. Director/IT/527484 Dated26/07/2024.

Notice Inviting Tender (NIT)

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

#	Description	Scrutiny Fee	Bid Security	Start date & Time for online Bid Downloading	End date & Time for online Bid Submission
1	Provisioning, Installation, Configuration, Testing, Commissioning, Operations & Maintenance of Information System for Enhancement of IT Security of BMC	Rs. 16,500/- + 9% CGST 9% SGST	Rs. 2,04,00,000/-	27.07 2024 at 11.00 hrs	21.08.2024 at 16.00 hrs
Note: Last date for online payment of Bid Security / Earnest money Deposit (EMD) is before due / end date & time for online Bid Submission prescribed above.					

5. The pre-bid meeting will be held on 05/08/2024 at 15.00 hours, at venue – Office of Director (IT), Basement, Extension Building, Municipal Head Office, 1, Mahapalika Marg, Fort, Mumbai – 400 001.
6. The prospective Bidder(s) should submit their suggestions/observations, if any, by email to director.it@mcgm.gov.in with a copy to manager01.it@mcgm.gov.in before 2 days of Pre-bid meeting. Only suggestions / observations received by email will be discussed and clarified in pre-bid meeting and any modification of the bidding documents, which may become necessary as a result of pre-bid meeting, shall be made by BMC exclusively through the issue of an addendum/corrigendum and shall be published on https://mahatenders.gov.in/nicgep/app.
7. Bidders shall note that any corrigendum issued regarding this E-Procurement notice will be published on the https://mahatenders.gov.in/nicgep/app portal only. No corrigendum will be published in the local newspapers.
8. The Bid document uploaded shall be read in conjunction with any addendum / corrigendum. A maximum of two authorized representatives of prospective Bidder(s), who have an authorization letter to attend the pre-bid meeting, can attend the pre-bid meeting and obtain clarification regarding specifications, works & Bid conditions.
9. The Bidder shall have to pay "Scrutiny Fee" through offline payment via challan to CFC (Citizen Facilitation Center) of BMC after bid submission end date and before commercial bid opening. In case of revision of the above-mentioned scrutiny fee, bidders shall pay revised scrutiny fee. The Bidder is required to be registered with BMC for further transactions in respect of the bidding process. The bidder

can register as a vendor with BMC using online application available at https://portal.mcgm.gov.in/irj/portal/anonymous/qlVendorApp

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

Sd/-

Director (IT)

Contents

Glossary

Sr. No.	Abbreviations and Acronyms	Expansion / Full Form / Explanation/Description	Sr. No.	Abbreviations and Acronyms	Expansion / Full Form / Explanation / Description
1	AMC	Additional Municipal Commissioner	31	ESIC	Employees' State Insurance Corporation
2	API	Application Programming Interface	32	FRS	Functional Requirement Specifications
3	BDS	Bid Data Sheet	33	GBPS	Gigabits Per Second
4	BEC	Bid Evaluation Committee	34	GCC	General Conditions of Contract
5	BI	Business Intelligence	35	GIGW	Government of India Guidelines for Websites
6	BMC	Brihanmumbai Municipal Corporation	36	GIS	Geographical Information System
7	CE	City Engineer	37	GRC	Governance, Risk & Compliance
8	CA	Current Assets	38	GST	Goods & Services Tax
9	CC (BDS Page 31)	Carbon Copy	39	HOD	Head of Department
10	CERT-In	Computer Emergency Response Team - India	40	HRM	Human Resource Management
11	CFC	Citizen Facilitation Centre	41	HTML	Hypertext Markup Language
12	CGST	Central Goods & Services Tax	42	HTTP	Hypertext Transfer Protocol
13	CL	Current Liabilities	43	HTTPS	Hypertext Transfer Protocol Secured
14	CMMi	Capability Maturity Model	44	HVAC	Heating Ventilation & Air Conditioning
15	COTS	Customizable Off-The-Shelf Software	45	ICT	Information & Communication Technology
16	CPD	Central Purchase Department	46	IDS	Intrusion Detection System
17	CPU	Central Processing Unit	47	IEEE	Institute of Electrical and Electronics Engineers
18	CRM	Customer Relationship Management	48	IIS	Internet Information Server
19	CSP	Cloud Service Provider	49	INR	Indian Rupee/s
20	CSS	Cascaded Style Sheet	50	IP	Internet Protocol
21	CSV	Comma Separated Values	51	IPR	Intellectual Property Rights
22	DBMS	Database Management System	52	IPS	Intrusion Prevention System
23	DC	Data Centre	53	IPv4	Internet Protocol Version 4
24	DMC	Deputy Municipal Commissioner	54	IPv6	Internet Protocol Version 6

25	DR	Disaster Recovery	55	IS	"Information System," means all the tools and managed services required to enhance IT security for BMC .
26	EDI	Electronic Data Interchange	56	ISO/IEC	International Standards Organization
27	EITM	Enterprise Information Technology Management	57	IT	Information Technology
28	EMC	Electromagnetic Compatibility	58	ITB	Instructions To Bidders
29	EMD	Earnest Money Deposit (Bid Security)	59	ITeS	Information Technology enabled Services
30	ERP	Enterprise Resource Planning	60	ITIL	Information Technology Infrastructure Library

Sr. No.	Abbreviations and Acronyms	Expansion / Full Form / Explanation/Description	Sr. No.	Abbreviations and Acronyms	Expansion / Full Form / Explanation / Description
61	JDBC	Java Database Connectivity	91	RTO	Recovery Time Objective
62	JPEG	Joint Photographic Experts Group	92	SD-WAN	Software-Defined Wide Area Network
63	JSON	Java Script Object Notation	93	SEI	Software Engineering Institute
64	JV	Joint Venture	94	SGST	State Goods & Services Tax
65	LDAP	Lightweight Directory Access Protocol	95	SIEM	Security Information & Event Management
66	LLP	Limited Liability Partnership	96	SITC	Supply, Installation, Testing & Commissioning
67	LOA	Letter of Acceptance	97	SLA	Service Level Agreement
68	LOI	Letter of Intent	98	SMS	Short Message Service
69	MBPS	Megabits Per Second	99	SOA	Service Oriented Architecture
70	MDM	Mobile Device Management	100	SOAP	Simple Object Access Protocol
71	MeitY	Ministry of Electronics & Information Technology	101	SQL	Structured Query Language
72	MMC Act 1888	Mumbai Municipal Corporation Act, 1888 (updated)	102	SSD	Solid State Drive
73	MSDG	Mobile Service Delivery Gateway	103	SSDG	State Service Delivery Gateway
74	NW	Net Worth	104	SSL	Secured Socket Layer
75	O&M	Operations & Maintenance	105	STQC	Standardization Testing & Quality Certification
76	OAT	Operational Acceptance Test	106	TA	Total Assets

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

Part I – Bidding Procedures

Section I - Instructions to Bidders

A. General

1. Scope of Bid

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

a. Throughout this bidding document:

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

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

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

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

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

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

2. Fraud and Corruption

a. The Bidders/Bidders and their respective officers, employees, agents, and advisers shall observe the highest standard of ethics during the Selection Process. Notwithstanding anything to the contrary contained in this RFB, the BMC shall reject a Proposal without being liable in any manner whatsoever to the Bidder, if it determines that the Bidder has, directly or indirectly or through an agent, engaged in corrupt practice, fraudulent practice, coercive practice, undesirable practice, or restrictive practice (collectively the “Prohibited Practices”) in the Selection Process. In such an event, the BMC shall, without prejudice to its any other rights or remedies, forfeit and appropriate the Bid Security or Performance Security, as the case may be, as mutually agreed genuine pre-estimated compensation and damages payable to the Authority for, inter alia, time, cost and effort of the Authority, in regard to the RFB, including consideration and evaluation of such Bidder’s Proposal.

b. Without prejudice to the rights of the BMC under Clause above and the rights and remedies which the BMC may have under the LOI or the Agreement, if an Bidder or Systems Supplier, as the case may be, is found by the Authority to have directly or indirectly or through an agent, engaged or indulged in any corrupt practice, fraudulent practice, coercive practice, undesirable practice or restrictive practice during the Selection Process, or after the issue of the LOI or the execution of the Agreement, such Bidder or Systems Supplier shall not be eligible to participate in any Bid or RFB issued by the BMC during a period of two years from the date such Bidder or Systems Supplier, as the case may be, is found by the BMC to have directly or through an agent, engaged or indulged in any corrupt practice, fraudulent practice, coercive practice, undesirable practice or restrictive practice, as the case may be.

The BMC requires that; bidders (applicants/proposers), consultants, contractors and suppliers; any sub-contractors, sub-consultants, service providers or suppliers; any agents (whether declared or not); and any

of their personnel, observe the highest standard of ethics during the procurement process, selection and contract execution of BMC-financed contracts, and refrain from Fraud and Corruption.

a. To this end, the BMC:

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

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

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

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

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

v. "Obstructive practice" is:

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

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

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

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

b. Rejects a proposal for award if the BMC determines that the firm or individual recommended for award, any of its personnel, or its agents, or its sub-consultants, sub-contractors, service providers, suppliers and/ or their employees, has, directly or indirectly, engaged in corrupt, fraudulent, collusive, coercive, or obstructive practices in competing for the contract in question.

c. In addition to the legal remedies set out in the relevant Legal Agreement, may take other appropriate actions, including declaring mis-procurement, if the BMC determines at any time that representatives of the BMC or of a recipient of any part of the proceeds of the project / subject work engaged in corrupt, fraudulent, collusive, coercive, or obstructive practices during the procurement process, selection and/or execution of the contract in question, without the BMC representative/s having taken timely and appropriate action satisfactory to the BMC to address such practices when they occur, including by failing to inform the BMC in a timely manner at the time they knew of the practices;

d. Pursuant to the BMC's Anti- Corruption Guidelines and in accordance with the BMC's prevailing sanctions policies and procedures, may sanction a firm or individual, either indefinitely or for a stated period of time, including by publicly declaring such firm or individual ineligible (i) to be awarded or otherwise benefit from a BMC-financed contract, financially or in any other manner; (ii) to be a nominated

sub-contractor, consultant, manufacturer or supplier, or service provider of an otherwise eligible firm being awarded a BMC-financed contract; and (iii) to participate further in the preparation or implementation of any BMC-financed project;

e. Requires that a clause be included in bidding/request for proposals documents and in contracts financed by BMC, requiring (i) bidders (applicants/proposers), consultants, contractors, and suppliers, and their sub-contractors, sub-consultants, service providers, suppliers, agents personnel, permit the BMC to inspect all accounts, records and other documents relating to the procurement process, selection and/or contract execution, and to have them audited by auditors appointed by the BMC.

3. Eligible Bidders

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

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

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

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

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

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

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

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

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

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

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

d. A Bidder that has been sanctioned/banned/blacklisted by the BMC, shall be ineligible to be prequalified for, initially selected for, bid for, propose for, or be awarded a BMC-financed contract or benefit from a BMC-financed contract, financially or otherwise, during such period of time as the BMC shall have

determined. The list of debarred firms and individuals is available at the office of Central Purchase Department of BMC.

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

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

4. Qualification of the Bidder

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

5. Code of integrity

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

a. prohibition of

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

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

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

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

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

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

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

   viii. making false declaration or providing false information for participation in a tender process or to secure a contract.

b. disclosure of conflict of interest.

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

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

B. Contents of Bidding Document

6. Sections of Bidding Document

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

b. **PART 1: Bidding Procedures**

i. Section I - Instructions to Bidders (ITB)

ii. Section II - Bid Data Sheet (BDS)

iii. Section III - Evaluation and Qualification Criteria

iv. Section IV – Bidding Forms

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

i. Section V - BMC's Project Requirements

1. Background and Informational Materials

2. Technical Requirements

3. Implementation Schedule

4. System Inventory Tables

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

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

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

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

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

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

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

c. The Bidder and any of its personnel or agents will be granted permission by the BMC to enter upon its premises and lands for the purpose of such visit, but only upon the express condition

that the Bidder, its personnel, and agents will release and indemnify the BMC and its personnel and agents from and against all liability in respect thereof, and will be responsible for death or personal injury, loss of or damage to property, and any other loss, damage, costs, and expenses incurred as a result of the inspection.

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

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

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

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

8. Amendment to the Bidding Document

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

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

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

C. Preparation of Bids

9. Cost of Bidding

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

10. Language of Bid

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

11. Documents Comprising the Bid

a. The Bid shall comprise the following:

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

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

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

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

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

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

vii. **Subcontractors:** list of subcontractors, in accordance with ITB - Documents Establishing Conformity of the Information System;

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

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

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

12. Letter of Bid and Price Schedule

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

13. Alternative Bids

a. Alternative Bids shall not be considered.

14. Documents Establishing the Eligibility and Qualifications of the Bidder

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

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

15. Documents Establishing Conformity of the Information System

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

b. The documentary evidence of conformity of the Information System to the bidding documents including:

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

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

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

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

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

c. References to brand names or model numbers or national or proprietary standards designated by the BMC in the bidding documents are intended to be descriptive and not restrictive. The Bidder may substitute alternative brand/model names or standards in its bid, provided that it

demonstrates to the BMC's satisfaction that the use of the substitute(s) will result in the Information System being able to perform substantially equivalent to or better than that specified in the Technical Requirements.

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

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

16. Bid Prices

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

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

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

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

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

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

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

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

17. Currencies of Bid and Payment

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

18. Period of Validity of Bids

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

b. In exceptional circumstances, prior to the expiration of the Bid validity period, the BMC may request Bidders to extend the period of validity of their Bids. The request and the responses shall be made in writing. If a Bid Security is requested in accordance with ITB – Bid Security, it shall also be extended for thirty days (30) beyond the deadline of the extended validity period. A Bidder may refuse the request without forfeiting its Bid Security. A Bidder granting the request shall not be required or permitted to modify its Bid.

19. Bid Security

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

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

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

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

e. The Bid Security may be forfeited:

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

   ii. if the successful Bidder fails to**:**

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

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

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

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

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

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

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

20. Format and Signing of Bid

a. The Bid shall be digitally signed by a person duly authorized to sign on behalf of the Bidder, using Digital Signature issued by authorized Certifying Authority. This authorization shall consist of written confirmation and shall be attached to the Bid. The name and position held by the person signing the authorization must be typed or printed below the signature. All scanned pages of the Bid where entries or amendments have been made shall be signed or initialed by the person signing the Bid and submitted on e-Tendering system of BMC.
b. In case the Bidder is a JV, the Bid shall be digitally signed by an authorized representative of the JV on behalf of the JV, and so as to be legally binding on all the members as evidenced by a power of attorney signed by their legally authorized representatives.

D. Submission and Opening of Bids

21. Submission of Bids

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

i. Folder 1 / Packet A – Letter of Bid, Documentary Evidence of Online Payment of Bid Security on e-Tendering System, Authorization, Bidder's Eligibility

ii. Folder 2 / Packet B – Documentary evidence of Qualifications and Conformity`

iii. Folder 3 / Packet C –Price Schedule to be duly filled in the online form of commercial offer on e-Tendering System of BMC. **Bidder shall NOT disclose the rates / prices quoted in any other Bid document.**

22. Deadline for Submission of Bids

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

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

23. Late Bids

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

24. Withdrawal, Substitution and Modification of Bids

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

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

25. Bid Opening

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

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

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

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

ii. the presence or absence of a Bid Security

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

E. Evaluation and Comparison of Bids

26. Confidentiality

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

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

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

27. Clarification of Bids

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

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

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

28. Deviations, Reservations, Omissions and Curable/Non-Curable Defect

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

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

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

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

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

      1. non-submission of following documents

         a. Valid Registration Certificate

         b. Valid Bank Solvency

         c. GST Registration Certificate

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

         e. Partnership Deed and any other documents

         f. Undertakings as mentioned in the tender document.

      2. Wrong calculation of Bid Capacity,

v. "Non-curable" Defect shall mean

1. In-adequate submission of EMD/ASD amount,
2. In-adequacy of technical and financial capacity with respect to Eligibility criteria as stipulated in the tender

29. Determination of Responsiveness

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

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

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

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

30. Nonconformities, Errors, and Omissions

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

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

31. Evaluation of Bids

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

b. **Preliminary Examination**

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

c. **Technical Evaluation**

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

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

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

d. **Economic (Commercial) Evaluation**

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

1. the Bid price, quoted by the bidder inclusive of all taxes, duties, levies and fees.

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

32. Comparison of Bids

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

33. Abnormally Low Bids

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

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

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

34. Eligibility and Qualification of the Bidder

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

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

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

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

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

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

F. Award of Contract

36. Award Criteria

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

   i. substantially responsive to the bidding document; and

   ii. the lowest evaluated cost.

37. Notification of Award

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

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

38. Signing of Contract

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

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

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

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

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

40. Performance Security

a. Within thirty (30) days of the receipt of the Letter of Acceptance from BMC, the successful Bidder shall furnish the Performance Security in accordance with the relevant GCC, using for that purpose the Performance Security Form included in Section – Bidding Forms. The Performance Security shall be valid for a period as mentioned **in BDS**.

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

41. Legal, Stationery Charges & Stamp Duty

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

b. Within thirty (30) days of the receipt of the Letter of Acceptance from BMC, the successful Bidder shall pay Stamp Duty, in accordance with the provisions of Article 63, Schedule I of Bombay Stamp Act 1958, using for that purpose the table given in Section – Bidding Forms or revised Stamp Duty Charges

published by the Government from time to time and effective on the date of issuance of the Notification of Award.

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

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

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

43. Grievance Redressal Mechanism

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

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

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

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

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

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

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

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

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

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

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

Determination of need of procurement

The decision of whether or not to enter into negotiations

Cancellation of a procurement process for certain reasons

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

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

44. Disclaimer

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

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

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

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

Section II - Bid Data Sheet (BDS)

ITB Clause No.	Information	Details
	A. General	
3.	Number of members allowed in JV/Consortium/Sub-Contracting	Joint Venture or Consortium will NOT be allowed to participate in the bidding for the subject work. If Sub-Contracting, Cost of sub-contractor shall not exceed 25% of Total Contract cost.
	C. Preparation of Bids	
18.	Bid Validity Period	180 Calendar Days from the Date of Submission of Bid
	D. Submission and Opening of Bids	
25.	Date, time, and venue of opening of Pre-qualification and Technical covers received in response to the E-Procurement Notice	22/08/2024 after 4 P.M. Office of Director (IT), Basement, Extension Building, Municipal Head Office, 1, Mahapalika Marg, Fort, Mumbai – 400 001
25.	Date, time, and venue of technical presentations by qualified bidders	(Date & Time will be decided and informed by BMC) Office of Director (IT), Basement, Extension Building, Municipal Head Office, 1, Mahapalika Marg, Fort, Mumbai – 400 001
25.	Date, time, and venue of opening of financial cover received in response to the E-Procurement Notice	(Date & Time will be informed after Technical Evaluation) Office of Director (IT), Basement, Extension Building, Municipal Head Office, 1, Mahapalika Marg, Fort, Mumbai – 400 001
	E. Evaluation and Comparison of Bids	
31.	Evaluation of Bids	BMC's evaluation of responsive Bids will take into account scored technical factors, in addition to cost factors. The technical factors are listed in Section III – Evaluation and Qualification Criteria Table 2 Evaluation of Technical Bid. Weight in percentage for Technical Factors – 70% Weight in percentage for Cost Factors – 30% The scoring methodology is specified in Section III Evaluation and Qualification Criteria.
	F. Award Criteria	
40.	Performance Security	10% of the contract value valid upto the entire contract period + 3 Months (including defect liability period or payment of final bill whichever is later), within 30 days from the date of the award of the contract or prior to signing of the contract whichever is earlier or as intimated in the notification of intention to award/work order issued by BMC.

Section III - Evaluation and Qualification Criteria

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

1. Evaluation of Prequalification

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

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

	[Net worth is required to be positive]		
2.2 Average Annual Turnover from System Integration Projects	Minimum average annual turnover of **400 Crore,** calculated as total certified payments received for system integration contracts in progress or completed, within the last three (3) years	Must meet requirement	Form – Average Annual Turnover from System Integration Projects, along with details of Extracts from the audited balance sheet and profit & loss; OR Certificate from the statutory auditor / Chartered Accountant
Factor	**3 Experience**		
3.1 General Experience	Experience under Network Security and Network Access Control System Implementation contracts at least 3 projects in the role of prime bidder for at least the last three [3] years prior to the applications submission deadline.	Must meet requirement	Form – General Experience
3.2.1 Specific Experience	The Bidder must have experience of successful Go-Live / completed project(s) during last five years (as on the last date of bid submission) in Central / State Government/Urban Local Bodies / Public Sector Companies / Banking Financial Services & Insurance (BFSI)/Enterprise Sector of below mentioned project value in India: Project shall include Network Security or Infrastructure Security or Cybersecurity or Network Access Control System Implementation contracts involving provisioning, and operations & maintenance of IT system as a prime bidder. 1. At least one project with a value not less than **80 Crore** **OR** 2. At least two projects with a value not less than **50 Crore** **OR** 3. At least three projects with a value not less than **40 Crore**	Must meet requirement	Form Specific Experience along with Completion certificates from the client; OR Work order + Self certificate of completion (Certified by the statutory auditor / Chartered Accountant); OR Work Order + Phase Completion Certificate from the client
3.2.2 Specific Experience IT	Bidder must have at least 10 certified OEM Engineers on proposed solution deployment.	Must meet requirement	Certification from OEM for each proposed solution deployment.

Personnel Experience			
3.2.3 Specific Experience SOC/NOC Operation	Bidder should have SOC & NOC operation in India / Global for last 3 years.	Must meet requirement	Form Specific Experience along with Completion certificates from the client; OR Work order + Self certificate of completion (Certified by the statutory auditor / Chartered Accountant); OR Work Order + Phase Completion Certificate from the client
Factor	**4 Certifications & Registrations**		
4.1 Certifications	Bidder have following certifications: - ISO 9001, ISO 27001, ISO/IEC 20000	Must meet requirement	Copy of the Valid Certificate signed and stamped by the Authorized Signatory of the Bidder.
4.2 GST Registration	Valid GST Registration and Income Tax Permanent Account Number (PAN)	Must meet requirement	Copy of GST registration number and PAN card
4.3 Cloud Empanelment	This criteria is applicable only for bidders offering fully or partially Cloud based solutions: - The CSP should be a MeitY Empaneled CSP (Cloud Service Provider) & STQC Audit Compliant.	Must meet requirement	Undertaking from the bidder on the letter head of the company, mentioning that CSP is a MeitY Empaneled and STQC Audit Compliant.
4.4 OEM Authorization	Bidder should be authorized by all OEMs.	Must meet requirement	Manufacturer Authorization Form (MAF) from all OEMs.

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

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

2. Evaluation of Technical & Commercial Bid

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

2.2. The BEC may require written clarifications from the Bidders to clarify ambiguities and uncertainties arising out of the evaluation of the Bid documents (to be stated precisely as it should be in BMC's interest). For more details, please refer ITB - Clarification of Bids.

2.3. In order to qualify technically, a Bid must secure a minimum of 75% of total marks in technical evaluation after summing up. Only those Bids which have a minimum score of 75% 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.

2.4. BMC reserves the right to lower the minimum required marks if none of the Bidders achieves 75% of the total marks.

2.5. Only the Bids qualifying the technical evaluation will be considered for commercial evaluation.

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

2.6.1. BMC shall appoint a Bid Evaluation Committee (BEC) to scrutinize and evaluate the pre-qualification, technical and commercial bids received.

2.6.2. The BEC will examine the Bids to determine whether they are complete, responsive and whether the bid format conforms to the bid requirements. BMC may waive any informality or non-conformity in a bid which does not constitute a material deviation according to BMC.

2.6.3. The bid prices should not be mentioned in any part of the bid other than the Commercial Bid.

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

2.6.5. The Technical Bids of only those Bidders, who qualify & meet all the criteria in the Pre-Qualification stage, shall be considered, and will be evaluated as per the evaluation criteria given in the section below by the Bid Evaluation Committee (BEC).

2.6.6. The BEC may require written clarifications from the Bidders to clarify ambiguities and uncertainties arising out of the evaluation of the Bid.

2.7. **Combined Evaluation (For Quality and Cost Based Selection – QCBS)**

BEC will evaluate and compare the Bids that have been determined to be substantially responsive. An Evaluated Bid Score (B) will be calculated for each responsive Bid using the following formula (for comparison in percentages), which permits a comprehensive assessment of the Bid price and the technical merits of each Bid:

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

where

C = Evaluated Bid Price

C_{low} = the lowest of all Evaluated Bid Prices among responsive Bids

T = the total Technical Score awarded to the Bid

T_{high} = the Technical Score achieved by the Bid that was scored best among all responsive Bids

X = weight for the Cost as specified in the BDS

The Bid with the best evaluated Bid Score (B) among responsive Bids shall be the Most Advantageous Bid provided the Bidder was prequalified and/or it was found to be qualified to perform the Contract.

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

#	Parameter	Evaluation Points	Max Marks	Documents required
1.	**General Experience** Experience under Network Security or Network Access Control System Implementation contracts at least 3 projects in the role of prime bidder for at least the last three [3] years prior to the applications submission deadline.	• 5 or more projects – 20 marks • 4 projects – 15 marks • 3 projects – 10 marks	20 marks	Form General Experience along with Completion certificates from the client; OR Work order + Self certificate of completion (Certified by the statutory auditor / Chartered Accountant); OR Work Order + Phase Completion Certificate from the client Bidder should also submit a certification from the client confirming the value of the project
2.	**Specific Experience** The Bidder must have experience of successful Go-Live / completed project(s) during last five years (as on the last date of bid submission) in Central / State Government/Urban Local Bodies / Public Sector Companies / Banking Financial Services & Insurance (BFSI)/ Enterprises Sector of below mentioned project value in India: Project shall include Network Security or Infrastructure Security or Cybersecurity or Network Access Control System Implementation contracts involving provisioning, and operations & maintenance of IT system as a prime bidder. 1. At least one project with a value not less than 80 Crore OR 2. At least two projects with a value not less than 50 Crore OR 3. At least three projects with a value not less than 40 Crore	• 80 Crore or more projects –20 marks • Between 50 Crore and 79 Crore projects– 15 marks • Between 40 Crore and 49 Crore projects – 10 marks	20 marks	Form Specific Experience along with Completion certificates from the client; OR Work order + Self certificate of completion (Certified by the statutory auditor / Chartered Accountant); OR Work Order + Phase Completion Certificate from the client Bidder should also submit a certification from the client confirming the value of the project
3.	**Specific Experience of Personnel / Manpower Resources: -** Bidder must have a minimum number of 200 IT personnel as on date of submission of bid on its roll out of which Bidder must have at least 10 IT	• 200 or above – 15 marks. • Between 150 to 199 – 10 marks. • Between 100 to 149 – 5 marks.	15 Marks	Employees State Insurance Corporation (ESIC) / Provident Fund (PF) certificate should be submitted for 200 IT

	Personnel OEM certified for each proposed technology solution.			Personnel and certification from OEM of 10 IT personnel for proposed technical solution.
4.	**Specific Experience of SOC/NOC operation in India/Global in last 3 years**	• SOC & NOC Operation- 8 Marks • SOC or NOC Operation- 4 Marks	8 Marks	Form Specific Experience along with Completion certificates from the client; OR Work order + Self certificate of completion (Certified by the statutory auditor / Chartered Accountant); OR Work Order + Phase Completion Certificate from the client
5.	**Bidder's Quality certifications**	• ISO 9001:2015, ISO 27001:2013- 7 Marks • ISO 9001, ISO 27001- 4 Marks	7 Marks	Bidders should submit certificates. These certificates should be valid as of date of this Bid submission
6.	**Empanelment**	• Cert-IN empanelment – 15 Marks	15 Marks	Documentary evidence for Cert-IN empanelment
7.	**Implementation Approach and Methodology:** - Every bidder will be given a timeslot of 60 minutes to demonstrate the proposed Information system implementation including design, configuration, operations and maintenance of applications on such platform.	Bidder should provide • Understanding of the project • Transition Plan • Technical Approach and Methodology • Solution Proposed • Project Plan • Capacity Building Plan • Exit Plan	15 Marks	Technical proposal and or Presentation as a part of technical bid

Section IV- Bidding Forms

1. Letter of Bid

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

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

To:

Department Office Address:

We, the undersigned, declare that:

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

2. Bidder Information Form

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

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

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

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

3. Bidder's JV / Consortium Members Information Form

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

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

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

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

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

DECLARATION CUM-INDEMNITY BOND

Date: dd/mm/yyyy

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

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

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

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

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

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

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

Dated _____ day of _____, 20__

Identified by me

Before me

Advocate

5. Historical Financial Performance

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

Page _____ of _____ pages

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

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

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

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

6. Average Annual Turnover

Bidder's Legal Name: _____ Date: _____
JV Member Legal Name: _____ RFB No.: _____
Page _____ of _____ pages

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

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

7. Experience - General Experience

Bidder's Legal Name: ______________________________ Date: ______________________

JV Member Legal Name: ______________________________ RFB No.: ___________________

Starting Month / Year	Ending Month / Year	Years*	Contract Identification	Role of Bidder
______	______		Contract name: Brief Description of the Information System performed by the Bidder: Name of Purchaser: Address:	_________
______	______		Contract name: Brief Description of the Information System performed by the Bidder: Name of Purchaser: Address:	_________
______	______		Contract name: Brief Description of the Information System performed by the Bidder: Name of Purchaser: Address:	_________
______	______		Contract name: Brief Description of the Information System performed by the Bidder: Name of Purchaser: Address:	_________
______	______		Contract name: Brief Description of the Information System performed by the Bidder: Name of Purchaser: Address:	_________
______	______		Contract name: Brief Description of the Information System performed by the Bidder:	_________

			Name of Purchaser: Address:	

8. Specific Experience

Bidder's Legal Name: _____ Date: _____

JV Member Legal Name: _____ RFB No.: _____

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

9. Financial Proposal Template

Covering letter

To:

<Location, Date>

<Name>

<Designation>

<Address>

<Phone Nos.>

<Fax Nos.>

<Email id>

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

Dear Sir/Madam,

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

1. PRICE AND VALIDITY

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

2. UNIT RATES

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

3. TENDER PRICING

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

4. QUALIFYING DATA

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

5. BID PRICE

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

6. PERFORMANCE BANK GUARANTEE

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

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

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

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

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

Yours sincerely,

Authorized Signature:

Name and Title of Signatory: Name of Firm:

Address:

10. Personnel Capabilities

Name of Bidder or partner of a Joint Venture

1.	Title of position
	Name of prime candidate

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

11. Candidate Summary

Name of Bidder or partner of a Joint Venture

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

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

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

12. Manufacturer's Authorization form

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

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

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

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

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

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

Signed _____

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

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

[add Corporate Seal (where appropriate)]

13. Subcontractor's Agreement

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

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

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

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

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

Signed _____

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

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

[add Corporate Seal (where appropriate)]

14. List of Proposed Subcontractors

#	Item	Proposed Subcontractor	Place of Registration & Qualificatio

15. Technical Capabilities

Name of Bidder or partner of a Joint Venture

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

16. Format of the Technical Bid

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

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

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

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

Technical Responsiveness Checklist

Sr. No.	Technical Requirement Details	Compliance Yes / No / Clarification if any

B	Functional, Architectural, Performance & Security Requirements	
1	Legal and Regulatory Requirements to be met by the Information System	
1.1	Data Protection and Privacy Laws:	
	Comply with applicable data protection and privacy laws if any.	Yes
	Implement appropriate security measures to protect personal and sensitive information stored in the Information System.	Yes
	Obtain necessary consent from individuals for the collection, storage, and processing of their personal data.	Yes
1.2	....	
1.3	...	

In demonstrating the responsiveness of its bid, the Bidder must use the Technical Responsiveness Checklist (Format as given above). Failure to do so significantly increases the risk that the Bidder's Technical Bid will be declared technically non-responsive. Among other things, the checklist should contain explicit cross-references to the relevant pages in supporting materials included the Bidder's Technical Bid.

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

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

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

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

17. Intellectual Property Forms

Notes to Bidders on working with the Intellectual Property Forms

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

18. Software List

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

19. List of Custom Materials

Custom Materials

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

(To be provided on the letter head of Bidder)

No……..… Date……

To

The……

Brihanmumbai Municipal Corporation,

Mumbai.

Subject: - Attending Pre-bid Meeting / Bid Opening

Reference: - Bid No…… due date…….

Sir,

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

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

Kindly permit him/her to attend the same.

Yours faithfully,

Signature:

Name of signatory:

Designation:

Rubber Stamp:

21. Pre-Bid Query Format

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

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

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

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

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

Table of Legal & Stationery Charges

Contract Value	Legal Charges + Stationery Charges
Up to INR 50,000 /-	Nil
From INR 50,001/- To INR 1,00,00,000/-	0.10% of contract cost (Rounding off such amount to next hundredth) plus 18% GST. Minimum INR 1,000/- + GST
From INR 1,00,00,001 /- To INR 10,00,00,000 /-	INR 10,000/- for contract value INR 1,00,00,000/- plus 0.05% of contract cost above INR 1,00,00,000/- (Rounding off such amount to next hundredth) plus 18% GST.
From INR 10,00,00,001 /- To further any amount	INR 55,000/- for contract value INR 10,00,00,000/- plus 0.01% of contract cost above INR 10,00,00,000/- (Rounding off such amount to next hundredth) plus 18% GST.

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

Stamp Duty Charges Payable By Successful Bidder

#	**Where the amount or value set forth in such contract does not exceed rupees ten lakh.**	**Five Hundred rupees stamp duty**
1	Where it exceeds rupees ten lakhs	Five hundred rupees plus 0.1% of the amount above rupees ten lakh subject to the maximum of rupees twenty-five lakh stamp duty.
2	Stamp Duty on Bank Guarantee	0.5% for the amount secured by Bank Guarantee subject to maximum of rupees ten lakh.

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

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

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

List of Approved Banks

The Performance Security (Bank Guarantee) issued by branches of approved Banks beyond Kalyan and Virar can be accepted only if the said Bank Guarantee is countersigned by the Manager of a Branch of the same Bank within the Mumbai City limit categorically endorsing thereon that the said Bank Guarantee is binding on the endorsing Branch of the Bank within Mumbai limits and is liable to be enforced against the said Branch of the Bank in case of default by the Supplier furnishing the Banker’s guarantee.

Nationalized Banks.		
Bank of Baroda	Bank of India	Bank of Maharashtra
Canara Bank	Central Bank of India	Indian Bank
Indian Overseas Bank	Punjab & Sind Bank	Punjab National Bank
State Bank of India	UCO Bank	Union Bank of India
Private Sector Banks.		
Axis Bank Ltd.	Bandhan Bank Ltd.	CSB Bank Ltd.
City Union Bank Ltd.	DCB Bank Ltd.	Dhanlaxmi Bank Ltd.
Federal Bank Ltd.	HDFC Bank Ltd	ICICI Bank Ltd.
Induslnd Bank Ltd	IDFC First Bank Ltd.	Jammu & Kashmir Bank Ltd.
Karnataka Bank Ltd.	Karur Vysya Bank Ltd.	Kotak Mahindra Bank Ltd
Lakshmi Vilas Bank Ltd.	Nainital Bank Ltd.	RBL Bank Ltd.
South Indian Bank Ltd.	Tamilnad Mercantile Bank Ltd.	YES Bank Ltd.
IDBI Bank Ltd.		
Scheduled Urban Co-op. Banks Licensed to issued Bankers Guarantee.		
Abhyudaya Co-Op. Bank Ltd.	Bassein Catholic Co-Op. Bank Ltd.	Bharat Co-Op. Bank Ltd.
Bombay Mercantile Co-Op. Bank Ltd.	Citizen Credit Co-Op. Bank Ltd.	Dombivli Nagari Sahakari Bank Ltd.
Greater Mumbai Co-Op. Bank Ltd.	Janakalyan Sahakari Bank Ltd.	Janata Sahakari Bank Ltd.
Kalyan Janata Sahakari Bank Ltd.	Kapol Co-Op. Bank Ltd.	Mahanagar Co-Op. Bank Ltd.
Mumbai District Central Co-Op. Bank Ltd.	NKGSB Co-Op. Bank Ltd.	New India Co-Op. Bank Ltd.
Parsik Janata Sahakari Bank Ltd.	Punjab & Maharashtra Co-Op. Bank Ltd.	Rupee Co-Op. Bank Ltd.
Sangli Urban Co-Op. Bank Ltd.	Saraswat Co-Op. Bank Ltd.	Thane Bharat Sahakari Bank Ltd.
Thane Janata Sahakri Bank Ltd.	The Cosmos Co-Op. Bank Ltd.	The Shamrao Vitthal Co-Op. Bank Ltd.
The Zoroastrian Co-Op. Bank.		
State Co-op. Banks.		
The Maharashtra State Co-Op. Bank.		
Foreign Banks.		
Australia and New Zealand Banking Group Ltd.	Westpac Banking Corporation	Bank of Bahrain & Kuwait BSC
AB Bank Ltd.	Sonali Bank Ltd.	Bank of Nova Scotia
Industrial & Commercial Bank of China Ltd.	BNP Paribas	Credit Agricole Corporate & Investment Bank
Societe Generale	Deutsche Bank	HSBC Ltd
PT Bank Maybank Indonesia TBK	Mizuho Bank Ltd.	Sumitomo Mitsui Banking Corporation
The Bank of Tokyo- Mitsubishi UFJ, Ltd.	Cooperatieve Rabobank U.A.	Doha Bank
Qatar National Bank	JSC VTB Bank	Sberbank
United Overseas Bank Ltd	Bank of China Ltd.	Shinhan Bank
Woori Bank	KEB Hana Bank	Industrial Bank of Korea
Kookmin Bank	Bank of Ceylon	Credit Suisse A.G
CTBC Bank Co., Ltd.	Krung Thai Bank Public Co. Ltd.	Abu Dhabi Commercial Bank Ltd.
Mashreq Bank PSC	First Abu Dhabi Bank PJSC	Emirates Bank NBD
Barclays Bank Plc.	Standard Chartered Bank	NatWest Markets Plc
American Express Banking Corporation	Bank of America	Citibank N.A.
J.P. Morgan Chase Bank N.A.	SBM Bank (India) Limited*	DBS Bank India Limited*

23. CONTRACT FORMS

Notes to the BMC on preparing the Contract Forms

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

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

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

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

Notes to Bidders on working with the Sample Contractual Forms

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

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

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

1. CONTRACT AGREEMENT

Request For Bids No…… Due on …/…/.….

Sanction No. …… Dated……

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

During the period from …….…… to ……..

Contract Cost:……

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

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

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

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

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

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

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

NOW IT IS HEREBY AGREED as follows:

Article 1. Contract Documents	1.1 Contract Documents (Reference GCC Clause (Definitions)) The following documents shall constitute the Contract between the BMC and the Supplier, and each shall be read and construed as an integral par of the Contract: (a) This Contract Agreement and the Appendices attached to the Contrac Agreement (b) Special Conditions of Contract (c) General Conditions of Contract (d) Technical Requirements (including Implementation Schedule) (e) The Supplier's bid and original Price Schedules (f) ***[Add here: any other documents]*** 1.2 Order of Precedence (Reference GCC Clause (Contract Documents)) In the event of any ambiguity or conflict between the Contract Documents listed above, the order of precedence shall be the order in which the Contract Documents are listed in Article 1.1 (Contract Documents) above provided that Appendix 7 shall prevail over all provisions of the Contrac Agreement and the other Appendices attached to the Contract Agreemen and all the other Contract Documents listed in Article 1.1 above. 1.3 Definitions (Reference GCC Clause (Definitions)) Capitalized words and phrases used in this Contract Agreement shall have the same meanings as are ascribed to them in the General Conditions o Contract.
Article 2. Contract Price and Terms of Payment	2.1 Contract Price (Reference GCC Clause (Definitions) and GCC Clause (Contract Price)) The BMC hereby agrees to pay to the Supplier the Contract Price in consideration of the performance by the Supplier of its obligations unde the Contract. The Contract Price shall be the aggregate of: ***[insert: amount in words], [insert: amount in figures],*** as specified in the Price Schedule. The Contract Price shall be understood to reflect the terms and conditions used in the specification of prices in the detailed price schedules including the terms and conditions of the associated Incoterms, and the taxes, duties and related levies if and as identified.
Article 3. Effective Date for Determining Time for Operational Acceptance	3.1 Effective Date (Reference GCC Clause (Definitions)) The time allowed for supply, installation, and achieving Operationa Acceptance of the System shall be determined from the date when all o the following conditions have been fulfilled: (a) This Contract Agreement has been duly executed for and on behalf o the BMC and the Supplier; (b) The Supplier has submitted to the BMC the performance security and the advance payment security, in accordance with GCC Clause (Securities); Each party shall use its best efforts to fulfill the above conditions for which i is responsible as soon as practicable. 3.2 If the conditions listed under 3.1 are not fulfilled within two (2) months from the date of this Contract Agreement because of reasons no attributable to the Supplier, the parties shall discuss and agree on a

equitable adjustment to the Time for Achieving Operational Acceptance and/or other relevant conditions of the Contract.

Article 4. Appendixes

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

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

APPENDIXES

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

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

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

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

Signed, Sealed and delivered

By ……..…..

Of ……..……

In the presence of Contractors

1) ……..……

2) ……..

Signed, Sealed and delivered

By ……..…..

in the presence of Director/ Dy. MC

1) ……..……

2) ……..……

The Common seal of the Municipal Corporation of

Brihanmumbai was affixed on this ……. Day of

…..…… 20…... in the presence of

(1) ……..……

(2) ...……..…… SEAL

two Members of the Standing Committee

of the Brihanmumbai Municipal Corporation

and in the presence of the Municipal Secretary.

……

Municipal Secretary

APPENDIX 1. SUPPLIER'S REPRESENTATIVE

In accordance with GCC Clause (Definitions), the Supplier's Representative is:

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

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

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

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

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

APPENDIX 2. ADJUDICATOR

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

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

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

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

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

APPENDIX 3. LIST OF APPROVED SUBCONTRACTORS

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

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

Item	Approved Subcontractors	Place of Registration

APPENDIX 4. CATEGORIES OF SOFTWARE

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

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

APPENDIX 5. CUSTOM MATERIALS

The follow table specifies the Custom Materials the Supplier will provide under the Contract.

Custom Materials

APPENDIX 6. REVISED PRICE SCHEDULES

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

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

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

2. DRAFT NON-DISCLOSURE AGREEMENT

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

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

By and between _____("BMC") and _("Supplier").

Whereas, BMC and Supplier have entered into an Agreement ("Agreement") effective _____; and for

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 andmaterials, 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 BMC'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, "BMC" shall include the officers, employees, agents, consultants, contractors and representatives of BMC.

c) The term, "Supplier" shall include the directors, officers, employees, agents, consultants, contractors and representatives of Supplier, 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, Supplier 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 BMC or any of the prospective clients of BMC except as necessary, under prior written intimation from BMC, in connection with the Project, and ensure thatany such copy is immediately returned to BMC even without express demand fromBMC to do so;

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

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

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

of the other party therefore.

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

3. **Onus.** Supplier 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 – "Protection of Confidential Information" of this Agreement shall not apply to any Confidential Information:

a) Which is independently developed by Supplier 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 Supplier; or

c) Which at the time of disclosure to Supplier was known to such party free of restriction and evidenced by documentation in such party's possession; or

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

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

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

6. **Need to Know.** Supplier shall restrict disclosure of such Confidential Information to itsemployees 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 thedisclosing 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 andpower to enter into this Agreement and perform their obligations hereunder.

10. **Dispute Resolution.** If any difference or dispute arises between the BMC and the Supplier in connection with the validity, interpretation, implementation or alleged breach of any provision of this Agreement, any such dispute shall be referred to the Hon. Municipal Commissioner, BMC before arbitration.
    a) The arbitration proceedings shall be conducted in accordance with the (Indian) 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 governedby 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 ofthe 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 Supplier shall not solicit or attempt to solicit BMC's employees and/or consultants, for the purpose of hiring/contract or to proceed to conduct operations/business similar to BMC with any employee and/or consultant of the BMC who has knowledge of the Confidential Information, without the prior writtenconsent of BMC. This section will survive irrespective of the fact whether there exists a commercial relationship between Supplier and BMC.
19. **Term.** Subject to aforesaid section - Survival, 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 BMC

Name:

Title

WITNESSES:

1:

2:

For Supplier

Name:

Title:

WITNESSES:

1:

2:

3. PERFORMANCE AND ADVANCE PAYMENT SECURITY FORMS

3.1 PERFORMANCE SECURITY FORM (BANK GUARANTEE)

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

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

(With Stamp duty of 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 ---------- (Name of the Bank and address) BANK incorporated under the English / Indian Companies Acts and carrying on business in Mumbai (hereinafter referred to as 'the bank' which expression shall be deemed to include its successors and assigns) of the first part –----------

---------- (Name of the Supplier)

Inhabitants carrying on business at ---------- (Supplier's Address)

in Mumbai under the style and name of Messers ----------(Name of the Supplier)

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

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

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

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

IN WITNESS WHEREOF

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

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

Address ----------

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

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

Address ----------

---

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

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

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

Address ----------

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

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

Address ----------

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

3.2 ADVANCE PAYMENT SECURITY

Bank Guarantee

_____

[Guarantor letterhead or SWIFT identifier code]

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

a. has used the advance payment for purposes other than toward delivery of Goods; or

b. has failed to repay the advance payment in accordance with the Contract conditions, specifying the amount which the Applicant has failed to repay.

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

_____
[signature(s)]

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

4 LETTER OF ACCEPTANCE

[letterhead paper of the BMC]

[date]

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

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

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

Authorized Signature: _____

Name and Title of Signatory: _____

Name of Organization: Information Technology Department, Brihanmumbai Municipal Corporation

Attachment: Contract

5. INSTALLATION AND ACCEPTANCE CERTIFICATES

5.1 INSTALLATION AND ACCEPTANCE CERTIFICATES

5.1 Installation Certificate

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

To: ***[insert: name and address of Supplier]***
Dear Sir or Madam:

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

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

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

For and on behalf of the BMC

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

5.2 OPERATIONAL ACCEPTANCE CERTIFICATE

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

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

Dear Sir or Madam:

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

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

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

For and on behalf of the BMC

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

6 CHANGE ORDER PROCEDURES AND FORMS

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

General

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

Change Order Log

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

References to Changes

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

Annexes

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

6.1 Request for Change Proposal Form

(BMC's Letterhead)

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

To: ***[insert: name of Supplier and address]***
Attention: ***[insert: name and title]***

Dear Sir or Madam:

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

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

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

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

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

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

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

Document or Drawing No. Description

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

8. Procedures to be followed:
   (a) Your Change Proposal will have to show what effect the requested Change will have on the Contract Price.
   (b) Your Change Proposal shall explain the time it will take to complete the requested Change and the impact, if any, it will have on the date when Operational Acceptance of the entire System agreed in the Contract.
   (c) If you believe implementation of the requested Change will have a negative impact on the quality, operability, or integrity of the System, please provide a detailed explanation, including other approaches that might achieve the same impact as the requested Change.
   (d) You should also indicate what impact the Change will have on the number and mix of staff needed by the Supplier to perform the Contract.
   (e) You shall not proceed with the execution of work related to the requested Change until we have accepted and confirmed the impact it will have on the Contract Price and the Implementation Schedule in writing.
9. As next step, please respond using the Change Estimate Proposal form, indicating the proposed approach for implementing the Change, all its elements, and will also address the points in paragraph 8 above pursuant to GCC Clause (Changes to the System). Your Change Estimate Proposal should contain a first approximation of the proposed approach, and implications for schedule and cost, of the Change.

For and on behalf of the BMC

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

6.2 Change Proposal Form

(Supplier's Letterhead)

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

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

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

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

Dear Sir or Madam:

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

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

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

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

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

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

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

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

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

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

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

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

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

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

For and on behalf of the Supplier

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

6.3 Change Order Form

(BMC's Letterhead)

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

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

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

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

Dear Sir or Madam:

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

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

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

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

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

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

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

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

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

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

For and on behalf of the Supplier

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

6.4 Application for Change Proposal Form

(Supplier's Letterhead)

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

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

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

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

Dear Sir or Madam:

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

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

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

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

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

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

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

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

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

For and on behalf of the Supplier

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

Part II – BMC's Requirements

Section V – BMC's Requirements

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

A. Background and Informational Materials

A.1 BACKGROUND

0.1 The BMC

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

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

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

0.2 The BMC's Business Objectives for the Information System

0.2.1 The primary objective of proposed IT Security System/s is to facilitate efficient and organized management of IT Security and Applications performance of BMC.

0.2.2 The proposed Information System is expected to provide the following benefits.

1. Identity & Access Management (IAM)
   - Ensures that only authorized individuals have access to certain resources.
   - Helps in maintaining compliance with regulations regarding data access and protection.
   - Streamlines user provisioning and deprovisioning processes.

2. Patch Management
   - Keeps systems updated with the latest security patches, reducing vulnerabilities.
   - Minimizes the risk of exploitation by cyber threats that target known vulnerabilities.
   - Ensures compliance with security policies and regulations.

3. IT Asset Management
   - Helps in inventorying and tracking all IT assets within the organization.
   - Enables efficient resource allocation and utilization.

- Supports better decision-making regarding hardware and software investments.

4. Network Access Control (NAC)
   - Controls and restricts access to the network based on predefined security policies.
   - Enhances network visibility and security posture.
   - Mitigates the risk of unauthorized access and potential data breaches.

5. Privileged Access Management (PAM)
   - Manages and secures privileged accounts and access to critical systems.
   - Reduces the risk of insider threats and unauthorized access.
   - Ensures accountability and auditability for privileged activities.

6. Active Directory Management
   - Centralizes user authentication and authorization within a network.
   - Simplifies user management tasks such as password resets and group policies.
   - Enhances security by enforcing access controls and group policies.

7. Vulnerability Management
   - Identifies and prioritizes vulnerabilities in systems and software.
   - Helps in patch prioritization and resource allocation for risk mitigation.
   - Improves overall security posture by proactively addressing vulnerabilities.

8. Endpoint Detection and Response (EDR)
   - Monitors and analyzes endpoint activities to detect and respond to security threats.
   - Provides real-time visibility into endpoint security events.
   - Helps in containing and remediating security incidents on endpoints.

9. Application Performance Monitoring (APM)
   - Monitors the performance and availability of applications.
   - Helps in identifying and resolving performance issues before they impact users.
   - Ensures optimal user experience and productivity.

10. Data Loss Prevention (DLP)
    - Prevents unauthorized access, sharing, or loss of sensitive data.
    - Helps in compliance with data protection regulations.
    - Protects intellectual property and confidential information from insider and external threats.
11. Packet Capture (PCAP) and Network Detection
    - Security and intrusion detection
    - Network performance tuning

These tools collectively contribute to building a robust and comprehensive IT security infrastructure, addressing various aspects of cyber threats and risk management within an organization.

Following are the expected outcomes from this project, categorized on the basis of BMC Department's services, BMC administrators and Citizens:

Citizens	BMC Department and Administration
• Faster and more reliable access to critical applications and services • Increase in user satisfaction by enhancing security, availability and performance	• Efficient management of IT resources • Enhance security, availability and performance. • Improve Production Support • Improved decision making and cost efficiency • Enhance automation and lesser manual intervention

0.3 Key Issues & Challenges faced by Stakeholders.

BMC in last few years has invested heavily in technology infrastructure to improve the efficiency and effectiveness of Information System service delivery. Though service delivery has improved, there are still many areas of improvements. Please refer below for the key issues and challenges faced by various stakeholders.

1. Issues faced by BMC Department and Administration

b. Identity & Access Management (IAM):
- Complexity in managing and synchronizing identities across multiple systems and platforms.
- Balancing security with user convenience and productivity.
- Ensuring timely user access provisioning and deprovisioning, especially in large organizations with high employee turnover rates.

b. Patch Management:
- Patch deployment causing system downtime or compatibility issues with existing software.
- Difficulty in prioritizing patches based on criticality and relevance to the organization's environment.
- Ensuring patches are applied uniformly across all systems and devices, including remote and mobile endpoints.

c. IT Asset Management:
- Difficulty in accurately tracking and managing a large number of IT assets distributed across different locations.
- Lack of integration and compatibility between asset management systems and other IT infrastructure components.
- Ensuring data accuracy and completeness in asset inventories, especially with frequent changes and updates.

d. Network Access Control (NAC):
- Balancing security requirements with user accessibility and flexibility.
- Integration challenges with existing network infrastructure and security tools.

- Ensuring consistent enforcement of access control policies across wired and wireless networks.

e. Privileged Access Management (PAM):
- Managing and securing privileged accounts without disrupting operational workflows.
- Balancing security controls with the need to grant privileged access for legitimate business reasons.
- Addressing insider threats and unauthorized access by privileged users.

f. Active Directory Management:
- Complexity in managing and securing a large and complex Active Directory infrastructure.
- Ensuring proper delegation of administrative tasks while maintaining security and compliance.
- Addressing security risks associated with misconfigurations, insider threats, and external attacks targeting Active Directory.

g. Vulnerability Management:
- Prioritizing vulnerabilities based on risk and potential impact to the organization.
- Managing the volume of vulnerabilities and the limited resources available for remediation.
- Ensuring timely patch deployment and vulnerability remediation across all systems and applications.

h. Endpoint Detection and Response (EDR):
- Detecting sophisticated and evolving threats that bypass traditional endpoint security measures.
- Balancing detection accuracy with false positives to minimize alert fatigue.
- Ensuring visibility and response capabilities for endpoints across diverse environments, including remote and mobile devices.

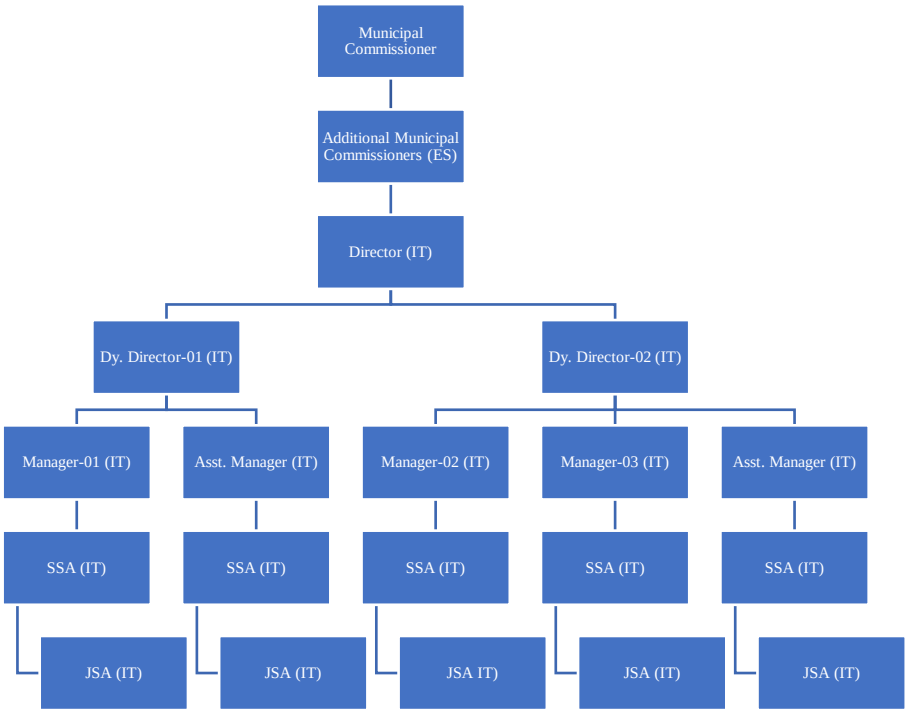
i. Application Performance Monitoring (APM):
- Identifying performance bottlenecks and issues across complex and distributed application environments.
- Balancing monitoring coverage with performance overhead and resource consumption.
- Ensuring correlation of performance data with business metrics and user experience.

j. Data Loss Prevention (DLP):
- Balancing data protection with the need for collaboration and data sharing within and outside the organization.
- Addressing challenges in accurately identifying and classifying sensitive data across diverse data repositories and formats.
- Ensuring DLP solutions are effectively deployed and configured to prevent data breaches without hindering legitimate business activities.

The Information system proposed by the Supplier should address the above issues.

0.4 Key Statistics of BMC DIT

0.4.1 Organization chart of department



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

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

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

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

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

A.2 INFORMATIONAL MATERIALS

0.1 Existing Information Systems / Information Technologies Relevant to the Information System

BMC at present has following IT security infrastructure implemented.

0.1.1 CISCO (Firewall)

0.1.2 CISCO (EDR)

0.1.3 Two Factor Authentication – Cymmetri (Domain)

0.1.4 CISCO Umbrella – DNS Base security

0.1.5 CISCO ISE (11,000 Licenses – not yet implemented)

0.1.6 Microsoft Active Directory (Windows 2019)

The Supplier is required to offer a comprehensive technical solution as per the requirements specified in this bid document that is compatible to function in tandem with the above mentioned infrastructure items. The Supplier may offer technical solution either using any free capacity available in the abovementioned infrastructure items or may offer a new technical solution. This will help BMC utilizing the capacity of it's already available IT security equipment to optimum level.

0.2 Stakeholders Roles and Responsibilities

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

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

- Developing a detailed project plan, including milestones, deliverables, and dependencies.
- Planning and coordinating the implementation project, including resource allocation, timelines, and risk management.
- Assigning tasks and responsibilities to team members, and tracking progress.
- Managing risks, issues, and changes throughout the implementation.
- Facilitating communication and collaboration among stakeholders.
- Reporting project status, including successes, challenges, and recommendations, to executive leadership.
- Overseeing the technical team and ensuring adherence to best practices and security standards.

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

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

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

B. Scope of Work

1. List of IT Security Services / Tools To Be Provided

The scope of work of the Supplier for the Information System includes the following: -

Provisioning (Subscription/Licenses), Design, Configuration, Testing, Commissioning, and Deployment of Information Systems listed in the table below-

The Supplier shall offer the IT Security Tools conforming the functions / features listed in the following table. Non-compliance to any of the technical and functional specification will attract rejection of the offer. Response except "Yes" or "No" is not acceptable. If any Bidder provides response other than "Yes" or "No", the same will be treated as Not Available i.e. "No".

No.	Name of Tool	Feature / Function	Description	Compliance (Yes/ No)
1	Microsoft Active Directory Management Tool	User and Group Management		
		- User Account Creation/Deletion	Allows administrators to create and delete user accounts.	
		- Group Management	Facilitates the creation and management of security and distribution groups.	
		Organizational Unit (OU) Management	Enables the creation and delegation of organizational units.	
		User Authentication and Authorization		
		- Password Management	Allows administrators to reset passwords and enforce password policies.	
		- Access Control	Manages user access rights through permissions and group memberships.	
		Group Policy Management		
		- GPO Management	Configures and applies group policies for controlling user and computer configurations.	
		- Policy Inheritance	Ensures that policies are inherited correctly across the AD hierarchy.	
		Active Directory Schema Management	Allows customization of the AD schema to extend attributes and classes.	
		Domain Controller Management		
		- Domain Controller Monitoring	Monitors the health and performance of domain controllers.	
		- Replication Management	Manages the replication of AD data between domain controllers.	
		LDAP Query and Search		

		- Advanced Search and Querying	Enables administrators to perform LDAP queries to retrieve specific information.	
		- LDAP Filter Creation	Allows the creation of complex LDAP filters for targeted searches.	
		Group and User Reporting		
		- Reporting Tools	Generates reports on AD objects, permissions, and usage.	
		- Audit Logging	Tracks changes to AD objects for security and compliance purposes.	
		Trust Relationship Management		
		- Domain Trust Configuration	Manages trust relationships between domains and forests.	
		Active Directory Recycle Bin	Allows recovery of deleted AD objects using the Recycle Bin feature.	
		Identity and Access Management (IAM) Integration	Works seamlessly with Identity and Access Management systems.	
		Security Configuration		
		- Security Settings Management	Configures and manages security settings for AD objects.	
		- Kerberos and NTLM Authentication Management	Configures authentication protocols for increased security.	
		Azure Active Directory Integration		
		- Sync Services	Integrates on-premises AD with Azure AD for a hybrid identity solution.	
		- Azure AD Application Management	Manages applications registered in Azure AD.	
		PowerShell Integration		
		- PowerShell Support	Provides PowerShell cmdlets for script-based management of Active Directory.	
		Multi-Forest and Multi-Domain Support	Allows administrators to manage AD resources in complex environments.	
		Role-Based Access Control (RBAC)	Enables delegation of specific tasks to other users or groups based on roles.	

		Alerts and Notifications		
		- Real-time Alerts	Notifies administrators of security events or policy violations.	
		- Notification Integration	Sends alerts via email, SMS, or integrates with other alerting systems.	
2	Application Performance Management Tool		- Application performance management system should monitor end-to-end performance and should cover following:	
			- User Experience monitoring	
			- Application, Database, and Component level monitoring	
			- Comprehensive Log monitoring and Analysis	
			- System should also offer analysis and diagnostics for root cause analysis of performance issues	
			- System should be able to notify users in real-time for any anomaly related to performance (high response, memory, CPU, etc.)	
			- System should offer unified and comprehensive dashboards for engineering teams as well as support analytics and reporting capabilities	
			- User experience monitoring should be able to monitor all sessions and specifically those sessions where users are facing issues. The system should offer user session capture and replay capability for further analysis and diagnostics.	
			- System should offer event generation capabilities on the client / browser / device side that helps identifying a struggling user. System should offer users to define and configure custom events	
			- System should offer funnel visualization and other analytics capabilities for improving performance.	
			- These capabilities should have but not be restricted to Real User Monitoring.	

			- The System should offer funnel comparison capabilities to understand and compare funnel / performance of business processes over the period of time	
			- The System should offer heat maps / click maps for optimizing page performance	
			- The System should offer form analytics for optimizing performance of pages that have forms	
			- The System should offer basic AB testing analysis to help identify improvements and optimizations in the pages of the application	
			- The System should offer Load-index based alerting capabilities besides offering static and moving baseline thresholds for alerts	
			- The System should offer comprehensive diagnostics and automated actions on alerts and triggers. These associated actions could be in form of:	
			- TCP Dump	
			- Thread Dump	
			- Heap Dump	
			- Run Command / Execute a Script	
			- The system should offer comprehensive server / application monitoring covering both system level as well as application level stats	
			- The system should be able to monitoring and trace individual transaction details.	
			- The system should offer auto discovery of business transactions.	
			- The system should offer server configuration-change monitoring.	
			- The system should offer end-to-end transaction tracing and ability to correlate user actions with events generated on the application stack layers	

			- The system should offer drill-down capabilities across layers – user experience, application layer, system layer, and logs.	
			- The system should be able to do comprehensive Log monitoring (system, application, DB logs, etc.) including access logs, errors logs, irrespective of type and format of logs	
			- The system should offer Automated query based log search and identification mechanism for logs related to a specific flow path or a specific business transaction in case of performance issues.	
			- The system should provide mechanism to understand trends from Logs using log analysis	
			- The system should not restrict data retention for specific period. There should not be any charges for data retention even after months or years (if supported by disk space).	
			- The system should be able to perform Synthetic monitoring / Availability testing	
			The system should be able to perform memory profiling for new memory allocations. Class level details like objects created per class, total allocation and class level stacktrace should be present.	
			The system should be able to identify classes causing memory leaks and detail the survived memory and survived object count. The system should also be able to provide stacktrace of the said classes along with showing survived memory per GC Cycle	
			The system should be able to perform mutex lock analysis to identify top blocking locks, top blocked threads and top blocking threads. For each of these, the system should provide stacktraces of the locks, the block and wait time.	

			The system should be able to dynamically add checkpoints in application code to capture critical information like variable values at the time of code execution, add custom logs, view stacktrace etc.	
3	IT Asset Management Tool		Tool should allow to dynamically create multiple classes of Configuration Items / Assets for categorization and logical grouping	
			Each Item Type in the tool must have a unique name and unique identifier (like asset ID)	
			Able to manage Annual Maintenance Contract (AMC) vendors, AMC and provide AMC notification	
			Tool should allow users to add Items for each Item Type using both manual add + CSV add option	
			Tool must store CI details including asset ID, asset lifecycle status, criticality, barcode no., serial no., Tag no., asset OEM, asset vendor, asset warranty/AMC, installation date, invoice no., part no., cost and purchase date.	
			Tool must have option to configure warranty / AMC pre-expiry notification alerts	
			CIs stored in the tool should have linking option with Customers, Incidents, vendors and Locations	
			Tool should provide option to Automatically download the Service assets from integrated EMS/NMS solution	
			Tool must have option to attach documents for each CI like Invoice Soft Copy, AMC soft copy etc.	
			Tool must have option to capture and store the entire history of each CI in chronological order with timestamps	
			Ability to provide an inventory of hardware and software applications on end-user desktops & laptops including information on processor, memory, OS, software etc.	
			Ability to configure inventory-data specific reports for target devices	
			Facility to track changes by maintaining history of an asset	

			All asset management operations should be via web-based GUI using any web browser	
			Record & Change: tool allow the creation and maintenance of configuration items (CIs), it should have options to record attributes (properties) such as serial numbers, version, location, cost, AMCs, Assignments, etc. tool should have option to add/ update data for multiple CIs at once using CSV or REST API calls	
			Classes & Categories: attributes (properties) of pre-defined CI classes be extended, Dynamically new CI classes be created and managed in the tool, allow the construction of a multi-layered CI classes hierarchy, all the input attributes can be created for each category of the assets, possible to configure attribute value restrictions (i.e. text masks, upper and lower boundaries etc.), dynamically create custom input forms for each Item type	
			Relations: CI's be linked via relations to create an end-to-end view, allow the CI relationships to be changed via graphical interface	
			Assignments: assigning CIs to responsible groups or individuals,	
			Lifecycle: tool should enable a flexible lifecycle status management for CIs (e.g. planned / ordered / in development / in test etc.), allow the creation of workflows that ensure that CIs are only changed by authorized changes.	

			support recording history of changes to CI records, support recording lifecycle history of CIs (history of related alerts, incidents, problems, changes, workorders etc.), should provide the lifecycle of financial value depreciation by using different methods ex. straight line depreciation.	
			Discovery: Agent Based discovery, Agent Less discovery of different types of assets like Router, Switch, APs, Fibre Optics devices, Firewall, Servers, VMs, Desktop, Hybrid Cloud Infraon, or any other type of IP enabled devices, additionally discovery solution integrated or is there a standard interface for connecting external discovery tools. discovery should support configurable reconciliation and deduplication rules.	
			Relations: individual relation types be configured and used in the tool and can they be specified individually (1:1, 1:n, n:m), tool facilitate documenting configurations by creating and customizing rules defining which types of relations are possible depending on which CIs are being linked. provide a graphical interface for the representation of the CIs and their relations	
			Search: possible to search for CIs based on a set of attributes, tool support creating views to quickly extract the necessary info about CIs based on different predefined filters or search conditions, graphical interface support filters defining which types of CIs and their relations to display to keep focus on the relevant configuration information	

			Audit:tool allow the creation of a configuration audit workflow, audit templates, random or scheduled audit for PAV, mobile application for scan and perform audit, recording audit results, facilitate prompt corrective actions based on audit results	
			Reports & Dashboard:Pre defined Asset Report & Dashbboard, Should have option to drag and drop dashboard configuration option Should have option to add multiple type of asset related widgets along with (Tabular, Summary, Multiple Graph options), Filter (predefined & Dynamic), Sort, Search, Group by, multi threshold, Export option to PDF , XLS etc., Generate automatically and send over Email or to a predefined folder, possible to define custom KPIs , A KPI definition must include the period-bound target value and the threshold value (to distinguish between the Green, Amber and Red zones).	
			Few KPIs for Assets:	
			Below are few simple KPI we can consider:	
			% of CIs under maintenance contract	
			% of CIs related to other Cis	
			% of CIs related to Services	
			Number of New Cis (Group by, Filter By Status)	
			Number of CIs Discovered	
			% Monitored Configuration Items	
			No., % CIs Ownership	
			Sum CIs Fault count/ Faulty Cis	
			Hardware CIs Missing Serial Number (Count,Filter by the Column)	
			Total model count (Group by Model/Columns)	

			Link a service request to asset management to validate items' availability. And create a process for unavailable items and link it to the procurement process	
			Able to manage Annual Maintenance Contract (AMC) vendors, AMC and provide AMC notification, option to configure warranty / AMC pre-expirty notification alerts	
			Tool must support Bar Code Generation, QR Code Generation for each Asset and Scanning through Application and update CMDB , CI using Mobile Application after scan	
			Asset GIS location Track & Tag using Mobile Application	
			Asset location update using QR code scanning	
			Should be able to calculate the GPS distance for the Base station to the destination for any asset (it will help to automate the billing)	
4	End point Detection & Recovery	Threat Detection and Prevention		
		- Real-time Threat Detection	Identifies and responds to security threats in real-time.	
		- Behavioral Analysis	Analyzes endpoint behavior to detect anomalies and threats.	
		- Signature-Based Detection	Identifies known malware based on predefined signatures.	
		Incident Response and Investigation		
		- Incident Logging and Tracking	Records and tracks security incidents on endpoints.	
		- Forensic Analysis	Conducts detailed investigation into security incidents.	
		- Threat Hunting	Proactively searches for threats on endpoints.	
		Endpoint Visibility and Monitoring		
		- Real-time Endpoint Monitoring	Monitors activities and events on endpoints in real-time.	

		- Endpoint Inventory	Maintains an up-to-date inventory of endpoint devices.	
		- User and Entity Behavior Analytics	Analyzes user behavior to identify suspicious activities.	
		Malware and Ransomware Protection		
		- Anti-Malware and Anti-Virus	Provides protection against malware and viruses.	
		- Ransomware Detection and Mitigation	Identifies and responds to ransomware attacks.	
		- Malicious URL and Email Protection	Blocks access to malicious URLs and attachments.	
		Firewall and Network Protection		
		- Host-Based Firewall	Controls incoming and outgoing network traffic on endpoints.	
		- Network Intrusion Detection System	Detects and responds to suspicious network activities.	
		- DNS Filtering	Blocks malicious domains and prevents DNS-based attacks.	
		Endpoint Remediation and Quarantine		
		- Automated Remediation	Automatically resolves or mitigates security incidents.	
		- Endpoint Isolation and Quarantine	Isolates compromised endpoints to prevent lateral movement.	
		- Threat Removal	Removes identified threats and malware from endpoints.	
		Security Policies and Configuration		
		- Policy Management	Defines and enforces security policies on endpoints.	
		- Configuration Compliance	Ensures endpoints adhere to security configuration standards.	
		- Device Control	Manages and controls device access to endpoints.	
		Integration with Security Systems		
		- SIEM Integration	Shares data with Security Information and Event Management systems.	

		- Integration with Threat Intelligence	Incorporates threat intelligence feeds for better detection.	
		- Integration with Identity Management	Collaborates with identity management systems for access control.	
		Reporting and Analytics		
		- Real-time Dashboards	Provides visual representations of endpoint security metrics.	
		- Incident Reports	Generates detailed reports on security incidents and responses.	
		- Trend Analysis	Analyzes trends in endpoint security over time.	
		Scalability and Performance		
		- Scalability Support	Scales to accommodate the number of endpoints in the environment.	
		- Minimal Performance Impact	Minimizes the impact on endpoint performance during scans.	
		User Education and Training		
		- Security Awareness Training	Offers training to end-users on security best practices.	
		- Phishing Simulation	Simulates phishing attacks to educate and assess user awareness.	
5	Network Access Control (NAC)	**Policy Enforcement**		
		- Access Policies	Defines rules and policies for controlling network access.	
		- Role-Based Access Control (RBAC)	Assigns access rights based on user roles.	
		Authentication Mechanisms		
		- Multi-Factor Authentication (MFA)	Requires multiple forms of authentication.	
		- Identity Provider Integration	Connects with identity management systems for user authentication.	
		Endpoint Compliance Checking		
		- Health Assessment	Evaluates the security posture and compliance of endpoints.	

			Users of unhealthy endpoints that do not meet compliance requirements, should receive a message about the endpoint status and instructions on how to achieve compliance	
		- Antivirus and Anti-malware Checks	Verifies security software on endpoints.	
			Endpoint posture and health checks should include Installed Applications,single AntiVirus and multiple AV, Firewall, Network Connections, Processes, Patch Management, Peer to Peer applications, Virtual Machines, USB Devices etc	
			Provide persistent agent for operating system to provide nonstop monitoring of the end point with automatic remediation and control	
			Offer web-based dissolvable agent for endpoint compliance check of personal and non IT-issued devices	
			Must be able to detect multiple network interfaces and Control it	
			Must be able to detect USB, disable it and remove it	
			Posture policy should support Configuration of time period for which posture Agent should ignore missing patches. Adminstration can able specify the grace period in hours, days, weeks, or months.	
			NAC solution should updated file check hash, health state for policy purposes, grace period in all health categories, client log uploads to remote server,Dashboard for posture request stats and MAC address randomization tracking/reporting	
		Guest Access Management		
		- Guest Networking	Facilitates secure access for guests and non-employee devices.	
			Guest access through captive portal with extensive branding and customization including company logos, visual imagery and optional advertisements with multimedia content to extend organization's messaging	
			Captive portal should have mobile device awareness to automatically size for smart phones, tablets and laptops	

			Guest self-registration through the web portal, delivering username and password directly to the visitor's Web browser, or sent via email or SMS.	
			Sponsor-based approval workflow to enable an internal employee to approve guest account before guest is allowed to access the network	
		- Guest Provisioning and Expiry	Automates guest access provisioning and expiration.	
			Customize guest access privileges to enforce bandwidth limits, access to specific resources, length of connections and set automatic account expiry after a specified number of hours or days	
			Guest portal shall have an option to accept Social logins using Facebook, Twitter, Slack and other social media credentials.	
			Third-party integration providing customizable workflows using rest-based API's for delivering streamlined registration and payment system integration	
		Network Visibility		
		- Device Discovery	Identifies and inventories devices on the network.	
		- Real-time Monitoring	Provides real-time visibility into network activities.	
		Integration with SIEM		
		- SIEM Integration	Shares data with Security Information and Event Management (SIEM) systems.	
		- Log Analysis	Analyzes logs to detect and respond to security incidents.	
		Automated Remediation		
		- Quarantine and Remediation	Automatically isolates non-compliant devices and initiates remediation.	
		- Automated Policy Enforcement	Enforces policies without manual intervention.	
		Device Profiling		
		- Fingerprinting	Profiles devices based on characteristics.	
			Provide automatic detection and categorization of endpoints for security and audit demands, regardless of device type,	

			using contextual data and use this data for optimizing access policies	
			Stored profiling data should identify device profile changes and dynamically modify authorization privileges. For example, if a printer appears as a Windows laptop, the system can automatically deny access. Should support Load balancing for profile scans and Scheduled Subnet scans	
			Support passive device profiling methods such as DHCP, Span Ports, HTTP User-Agent, MAC OUI and TCP SYN-ACK handshakes	
			Support active device profiling methods such as SNMP, Subnet Scan, SSH, Sflow, WMI and NMAP Scan.NAC solution should support profile Load balancing for profile scans, IPFIX support.	
			Support the following operating systems and versions: Microsoft Windows 11 and above, Apple macOS 10.10 and above	
			Provide automatic detection and categorization of endpoints for security and audit demands, regardless of device type, using contextual data and use this data for optimizing access policies	
			Stored profiling data should identify device profile changes and dynamically modify authorization privileges. For example, if a printer appears as a Windows laptop, the system can automatically deny access. Should support Load balancing for profile scans and Scheduled Subnet scans	
			Internal device fingerprint dictionaries that provide a way to automatically or manually update periodically. Capable to define custom fingerprints for wired and wireless devices	
		- Behavior Analysis	Analyzes device behavior to detect anomalies.	
		Personal Device (BYOD) Management		

			Automatically configure and provision mobile devices such as Windows, macOS, iOS, Android, Chromebook, and Ubuntu, enabling them to securely connect to enterprise network. Support for atleast 1000 users on day one. Each user can have upto two devices and support Sponsor approval required option for Onboarding.	
			Support the distribution of in-built CA generated certificates to third-party applications using SCEP and EST (RFC 7030) protocols.	
			Ensure rapid revocation and deletion of certificates for specific mobile devices if a user leaves the organization or the mobile device is lost or stolen.	
			Support Online Certificate Status Protocol (OCSP)	
			Capable to define the number of devices that can be on-boarded per user and validity of their certificates	
			Automatic device certificate provisioning/installation with sponsor approval required option for onboarding	
			Certificate Provisioning must work even after failover of its nodes	
			Must support Oauth and SAML 2.0 Identity Provider, which allows seamless single sign-on (SSO) to the cloud or on-premise applications.	
			Must support multiple multi-factor authenticatiors (MFA/2FA) such as Kasada, DUO, Imageware etc.	
			Should support Secure certificate based onboarding and Automatic device certificate provisioning / installation	
		Network Segmentation		
		- Micro-Segmentation	Divides the network into smaller segments for security.	
		- VLAN Support	Implements Virtual LANs (VLANs) for traffic isolation.	
		Integration with Endpoint Security Solutions	Integrates with endpoint security tools.	
		Integration with MDM		

		- Mobile Device Management (MDM)	Manages security policies for mobile devices.	
		Compliance Reporting		
		- Audit Trails	Generates detailed logs for compliance audits.	
		- Compliance Reports	Provides reports on adherence to security policies.	
		Scalability		
		- Support for Large Networks	Scales to accommodate the size and complexity of networks.	
		Policy-Based Enforcement		
		- Dynamic Policy Enforcement	Adjusts access policies based on changing network conditions.	
		User Authentication Integration		
		- Integration with LDAP/AD	Utilizes existing user directories for authentication.	
		- Single Sign-On (SSO) Support	Streamlines authentication processes.	
		Alerts and Notifications		
		- Real-time Alerts	Notifies administrators of security events or policy violations.	
		- Notification Integration	Sends alerts via email, SMS, or integrates with other alerting systems.	
			Predefined templates for reporting must be available	
			A reporting option must be available to provide a method for delivering validated templates to unique requirements in a timely manner.	
			Understanding trends, compliance and forensic analysis requires the ability to generate reports on data from selectable time frames in the past as well as on current data i.e Specific date and time range	
			In order to provide the information needed to make decisions and minimize data overload reporting systems must provide robust filtering options.	
			Must have support for notifications via Email	
			Web-based user interface that simplifies policy configuration, monitoring and troubleshooting	

		Authentication, Authorization and Accounting (AAA)		
			Integrated scalable AAA services (authentication, authorization, and accounting) including access policy management with a complete understanding of context, such as user's role, device type, location, time of day etc.	
			User and device authentication based on 802.1X, and Web Portal access methods across multi-vendor wired networks , wireless networks, and VPNs	
			Usage of multiple authentication protocols concurrently, such as PEAP, EAP-FAST, EAP-TLS, EAP-TTLS, and EAP-PEAP-Public	
			Must support RADSEC protocol to support RADIUS datagrams over TCP and TLS	
			Must be supplied with fine-grained control using attributes from multiple identity stores, such as Microsoft Active Directory, Kerberos, LDAP-compliant directory, Open Database Connectivity (ODBC)-compliant SQL database, token servers, and internal databases across domains within a single policy from day one	
			Non-802.1X devices (such as printers, IP phones, IP cameras and IOT devices) can be identified as known, based on the presence of their MAC addresses in database, or unknown upon connecting to the network.	
			Integrated TACACS+ server for secure authentication of device administrators, operators etc. with varied privilege levels. It should keep a track of the changes made by the logged-in user.	
			NAC solution should support reporting with manual or scheduled reports in PDF/CSV/xls formats, inventory dashboard showing details of learned devices, real-time monitoring of access requests and events, proactive alerts through Email	
			HTTP/RESTful API's, syslog messaging and Extensions capability to exchange endpoint attributes with firewalls, SIEM, endpoint compliance suites and other solutions for enhanced policy management	

			Mobile Device Management Integration to fetch information such as device manufacturer, model, OS Version, Jail-broken, presence of any black-listed application, MDM Agent installation status etc. and use this information in access policies	
			API Integration with helpdesk software allowing dynamic creation of problem tickets of any network triggered policy breaches	
			Inbuilt utilities for interactive policy simulation and monitor mode for assessing the policies before applying to the production network	
			Process inbound threat-related events (which are Syslog events received from any third-party vendor device, such as Firewall, SIEM) and perform enforcements and actions based on the defined enforcement policies and services.	
			Must have Multi domain AD support	
			All the user machines must be evaluated before allowed on the network and thus must only deploy with a secured IEEE 802.1X architecture . NAC solution must support deny access policy first.	
			NAC solutiuon should support Multivendor. Should have third party integration from day one.Should support automatic HA failover and Auto Upgrade tools NAC solution should use 802.1x authectication using native client of operating system	
			NAC solution should support Per policy based Certificate,Multifactor Authentication using MFA tool.	
		Requirement Summary		
			Hardware appliance or Virtual Appliance (Automatic HA failover) with 1:1 or N:1 redundancy . If Virtual Appliance is proposed, it shall be offered with OEM recommended Hardware/VM Hypervisor. There must be dedicated appliance for Reporting.Each Harware/Virual sofyteare should support 50000 concurrent connection.	
			Licenses supporting minimum 3500 concurrent sessions for AAA, Endpoint posture check, and TACACS+ on Day 1	

			5-Year 24x7 Hardware and Software Warranty with perpetual licenses. If it is not possible to offer perpetual licenses, the solution must include atleast 10 years of licensing upfront	
		OEM and Product Eligibility/Compliance		
			The solution shall be Common Criteria certified for network access control (NAC) solution, under both the Network Device collaborative Protection Profile (NDcPP) and the Extended Package for Authentication Servers modules. The certificate shall be attached as reference	
			OEM shall have R&D facility in India; if required site visit shall be arranged	
			OEM shall be capable of providing direct onsite warranty service for the products procured. The warranty service datasheet shall be attached with the proposal	
6	Patch Management	Patch Deployment		
		- Automated Patch Deployment	Automatically deploys patches to endpoints.	
		- Manual Patch Deployment	Allows administrators to manually deploy patches when needed.	
		- Scheduled Patching	Sets specific times for patch deployment to minimize disruptions.	
		Patch Assessment and Scanning		
		- Vulnerability Scanning	Identifies vulnerabilities in software and applications.	
		- Asset Inventory	Maintains an inventory of software and systems to assess patch status.	
		- Compliance Checks	Verifies compliance with security and patching policies.	
		Patch Rollback		
		- Rollback Mechanism	Allows the rollback of patches in case of issues or conflicts.	
		- Restore Points	Creates restore points before patch deployment for easy rollback.	
		Reporting and Analytics		
		- Patch Status Reports	Generates reports on the status of applied patches.	
		- Compliance Reports	Provides reports on compliance with patching policies.	

		- Trend Analysis	Analyzes trends in patching and vulnerabilities over time.	
		Integration with Vulnerability Management Systems	Integrates with vulnerability assessment tools for comprehensive security.	
		Automation and Workflow		
		- Workflow Automation	Automates patch approval and deployment workflows.	
		- Customizable Approval Processes	Defines custom processes for approving and testing patches.	
		Alerts and Notifications		
		- Real-time Alerts	Notifies administrators of critical vulnerabilities and patches.	
		- Notification Preferences	Allows customization of notification methods and preferences.	
		Patch Testing Environment		
		- Test Environment Integration	Integrates with testing environments to assess patch impact.	
		- Sandbox Testing	Provides a safe environment for testing patches before deployment.	
		Patch Rollout Control		
		- Staged Deployment	Deploys patches in stages to minimize impact and monitor for issues.	
		- Bandwidth Control	Controls bandwidth usage during patch deployment to prevent network congestion.	
		Supported Platforms and Applications		
		- Cross-Platform Support	Supports patching across various operating systems.	
		- Third-Party Application Patching	Manages patches for third-party applications and software.	
		Patch Catalog Management		
		- Patch Catalog Updates	Regularly updates the patch catalog to include the latest patches.	
		- Custom Patch Catalogs	Allows the creation of custom catalogs for specific needs.	
		Security Patching		

		- Critical Security Patching	Prioritizes and deploys critical security patches promptly.	
		- Zero-Day Vulnerability Response	Provides rapid response to emerging zero-day vulnerabilities.	
		Role-Based Access Control (RBAC)		
		- Delegation of Patch Management Tasks	Allows delegation of patch-related tasks based on roles.	
		Scalability and Performance		
		- Scalability Support	Scales to accommodate the size and complexity of the IT environment.	
		- Minimal Performance Impact	Minimizes impact on endpoint performance during patching.	
		Cloud Patch Management		
		- Cloud-Based Patching	Manages patch deployment for endpoints in cloud environments.	
		- Hybrid Cloud Support	Supports both on-premises and cloud-based patch management.	
7	Identity & Access Management (IAM)	Self-service including password reset and account unlock		
			Enables users to reset their forgotten LDAP / AD domain passwords and unlock their locked-out accounts without admin intervention. Users should be able to reset their password from-	
			A web browser using the proposed Information System's user portal.	
			The logon screens of Windows machines using the proposed Information System's login agent	
			A mobile device using the proposed Information System's mobile browser portal.	

			Enable users to request for application access through a portal / user interface for life time access or time based access	
			Users can view all the applications entitled to them along with the role provided, and where allowed, can SSO to the entitled applications	
			Users can request for change of role and request for additional roles	
			Users can request for access on behalf of other users	
			Users can delegate access to other users if allowed	
		Password Management		
			Password Synchronization	
			The system should allow users to synchronize their LDAP / AD domain password across their user accounts integrated on Premises and cloud applications like Microsoft 365.	
			Password policy enforcer The proposed Information System should be able to set Advanced password policy controls for an organization in addition to the native domain and fine-grained password policies offered by AD. These advanced password policies should be able to be used to set password controls that are not available in the native policies like:	
			Restriction of character repetition of consecutive characters from usernames and old passwords.	
			Restriction on the usage of weak passwords, dictionary words, and palindromes.	
			Password expiration notification	

			Password expiration notifications should be sent through email and SMS. The proposed Information System should allow sending multiple reminder notifications on specific days leading to the expiration.	
		Enterprise single sign-on (SSO)		
			Reduce the number of logins performed by the user by enabling enterprise SSO for Security Assertion Markup Language (SAML) applications like Microsoft 365.	
			System should allow configuration of standards based authentication principles such as SAML and OpenIDConnect.	
			System must support ability to integrate with custom applications including legacy built applications and make the authentication process SSO compliant.	
			System should support SSO integration of legacy applications where changes to that application are not possible due to any reason	
			System must support additional factor authentication during SSO (MFA or 2FA) where the user may be attempting to authenticate from an external system	
			Federated authentication of users should be supported during SSO	
		Multi-factor authentication (MFA)		
			MFA improves security through additional layers of identity verification along with the existing credential-based authentication. Proposed Information System should implement additional identity verification steps for the following:	

			Self-service password reset and account unlock.	
			Local Windows Machines and VPN Logins (where the VPN software supports Radius protocol)	
			Multifactor options must have	
			Mobile native applications for Time based OTP (TOTP) supporting Apple iOS and Android devices	
			The system should support various authentication techniques including biometrics such as fingerprint and facial recognition, Microsoft Authenticator, Google Authenticator (TOTP), and Security Questions and Answers.	
			The system should also support adaptive authentication including context-based access through geographic location based, Network reputation based, time anomaly based, device based.	
			The system should have support for FIDO principles	
			The system should allow a configurable mechanism for selecting the appropriate authentication policy and MFA options for users	
		User Life Cycle Management		
			The system must support the UCLM process-joiner, mover, leaver to provide access to enterprise users to organization resources	
			The system must support integration of multiple source of truth systems such as HRMS, AD / LDAP, data from flat files, fetch data from different database types	

			The system must support the reconciliation of identity records between two systems and consolidate the identity records across applications. In case records do not confirm, system must provide a report of such records	
			The system must allow synchronization of user attributes from source to target applications as per the need	
			The system must support creation of additional fields to sync the user attributes. There shall be no limit to the custom fields in the system.	
			The system must support automated provisioning of users to enterprise applications. Support for birthright access is required	
			The system must provide mechanism for role based access (RBAC) to enterprise applications where attributes of the user can define the access grants during creation and update of user events	
			The system must automatically disable the user identities in target applications when the user has left the organization	
			Workflow Management	
			The system must allow configuration of access approval matrix for application access through requests	
			The system should allow configuration of workflows for access such as Provisioning, De-provisioning, Role based request approval, Approval for system access and any such relevant access to organization resources	
		Governance of Identities		

			The system must support the ability to perform periodic access certifications for all or selected users	
			The system must have configurable options to remove access immediately or trigger a workflow when user's access is marked as revoked by the approver	
			The system must allow ability to setup the organization policies for segregation of duty	
			The system must provide mechanism for defining conflicting roles and understand the toxic role combinations	
			The system must automatically disable the user identities in target applications when the user has left the organization	
			The system should have option to show recommendation for approval of access requests governance certification	
			The system should have option to show recommendation for approval of certification requests	
		Passwordless Authentication		
			System must support the ability for users to authenticate without the requirement of passwords	
			The system must support all of the below options for passwordless authentication-	
			Consent based authentication	
			Biometric based authentication on supported devices	
			ToTP based authentication	
			OTP (SMS) based authentication	
		Adaptive Authentication		

			Automate access decisions to organizational resources using risk factors such as IP address, time of access, the device used, and the user's geolocation.	
			The system should have ability to detect through the use of an end-point agent, the device context and risks such as anti-virus definitions not up to date, missing patches, root-kits on the end-points	
			The system should be able to detect impersonation through different means and stop the access or require an additional factor (MFA) before allowing user to access	
			The system should have ability to alert the user and administrators where access is suspicious in nature	
			The system should option to check device compliance and based on configured policies allow access to the organizatio resources e.g. if system doesn't have antimalware system then user cant access financial transaction system	
		System Administration		
			The system must provide different role based access to administer different aspects of the system	
			All access for the administrators must be logged including all events performed by them in the system. The authentication of the administrative users must have 2FA enforcement.	
			The system must have pre-configured templates or settings and all pre-defined settings must enforce the highest security principles for risk management	

			All system configuration options and their settings must be documented and copy of the document must be accessible at any point in time	
			The system must support extending the use cases through the use of web-hooks which can be configured from the frontend	
			The system should support the delegation of administrative functions and also support decentralized administrative grants to specific users	
		Auditable events and Reports		
			The system must record all events performed by users or through any backend activity with the ability to understand who or what triggered it, from where, for what reason and how it was accessed.	
			Audit logs must be immutable and cannot be changed by any user / system event by any means.	
			The event log information should be exportable using APIs to any SIEM or EDR / XDR system. The system may also provide log data in syslog	
			The system must provide reports for all events relating to the identity and access management of the organization	
			The administrators should have a dashboard to view the activities of the system and understand in depth any event that requires investigation	
			The system should provide for reports to be exported / mailed from the system and the admin can schedule sending of specific reports as per need	
			Identity Risk Profiling	

			CISO Dashboard	
			Rapid AI/Ml based Rest API integration	
			The system should have option to define identity risk profile automatically with internal data as well as integration with SIEM	
		Integration and management		
			The system must provide out of box connectors / integration with standard systems such as HRM systems, Active Directory, Helpdesk / ITSM platforms	
			The system must have support for integration with different technology backends such as application languages (such as Java, Python, PHP, Dot Net, Golang, etc.), databases (such as Oracle, PostgreSQL, MSSQL, MySQL, MongoDB, DB2, etc.) and web-services frameworks such as REST, SOAP, GRAPH, etc.	
			The system must support the ability to integrate home grown, bespoke applications which may not support standard integration options	
		System performance		
			The system must be configured in high-availability mode with redundancy. There must not be any single point of failure of the system.	
			The system must utilize the strongest possible methods for ensuring confidentiality, integrity and availability as part of its design and system architecture	
			The system must adhere to best architecture patterns such as multi-tiered architecture	

			The system should support containerization for all components and such containers could be deployed and managed through any of the following - docker compose, Kubernetes or OpenShift for orchestration.	
			Every request to and from the system must be verified with industry best practices. Example JWT validations	
			The system must be horizontally and vertically scalable in all aspects. No component should be setup or configured that may hinder the performance of the system	
8	Privilaged Access Management (PAM)	Identity and Access Management		
		- Privileged Identity Management (PIM)	Manages and monitors privileged identities.	
		- Identity Verification and Authentication	Ensures secure access through strong authentication methods.	
		Privilege Elevation and Delegation		
		- Just-In-Time Privilege Elevation	Grants elevated privileges for a specific time window.	
		- Role-Based Access Control (RBAC)	Assigns privileges based on predefined roles and responsibilities.	
		Session Monitoring and Recording		
		- Real-time Session Monitoring	Monitors privileged sessions in real-time.	
		- Session Recording	Records and stores activity during privileged sessions.	
		- Playback and Forensic Analysis	Allows review and analysis of recorded session activities.	
		Credential Management		

		- Secure Password Storage	Safely stores and manages privileged account credentials.	
		- Password Rotation and Policy	Enforces regular password changes and adherence to security policies.	
		- SSH Key Management	Manages and rotates SSH keys used for authentication.	
		Access Request and Approval		
		- Access Request Workflow	Defines processes for requesting and approving privileged access.	
		- Multi-Step Approval Processes	Allows multi-tiered approval for sensitive access requests.	
		Integration with Identity Systems		
		- Integration with IAM Systems	Integrates with Identity and Access Management solutions.	
		- Single Sign-On (SSO) Support	Facilitates seamless access to privileged accounts.	
		Session Termination Controls		
		- Automatic Session Timeout	Terminates inactive privileged sessions automatically.	
		- Emergency Session Termination	Allows immediate termination of sessions in case of security incidents.	
		Audit Trails and Compliance		
		- Audit Logging and Reporting	Captures and logs privileged access events for auditing.	
		- Compliance Reporting	Generates reports for regulatory compliance requirements.	
		Alerts and Notifications		
		- Real-time Alerts	Notifies administrators of suspicious or unauthorized activities.	
		- Notification Integration	Sends alerts via email, SMS, or integrates with other alerting systems.	
		Endpoint Security Integration		
		- Integration with Endpoint Protection	Collaborates with endpoint security solutions for comprehensive protection.	
		API Support and Integration		

		- APIs for Integration	Provides APIs for integration with third-party applications and tools.	
		- Integration with SIEM Systems	Shares privileged access data with Security Information and Event Management systems.	
		Passwordless Authentication		
		- Biometric Authentication	Supports biometric methods for passwordless access.	
		- Multi-Factor Authentication (MFA)	Enhances security with multiple authentication factors.	
		Emergency Access Procedures		
		- Break Glass Procedures	Defines emergency procedures for accessing privileged accounts in critical situations.	
		- Dual Control Authentication	Requires two authorized individuals for critical operations.	
9	Vulnerability Management	Vulnerability Scanning		
		- Automated Vulnerability Scans	Conducts regular scans to identify vulnerabilities.	
		- Scheduled Scanning	Allows for scans to be scheduled at specific intervals.	
		- On-Demand Scanning	Permits ad-hoc scans for immediate vulnerability assessment.	
		Asset Discovery and Inventory		
		- Automatic Asset Discovery	Identifies and inventories assets on the network.	
		- Asset Tagging and Categorization	Organizes assets into categories for better management.	
		- Asset Criticality Assessment	Evaluates the criticality of assets based on their importance.	
		Vulnerability Assessment and Analysis		
		- Vulnerability Identification	Detects and categorizes vulnerabilities on assets.	
		- CVSS Scoring	Assigns Common Vulnerability Scoring System scores to vulnerabilities.	
		- False Positive Reduction	Minimizes false positives through accurate identification.	

		Patch Management Integration		
		- Integration with Patch Management Systems	Collaborates with patch management tools for comprehensive remediation.	
		- Patch Prioritization	Prioritizes patches based on criticality and impact.	
		Risk Assessment and Prioritization		
		- Risk Scoring	Calculates risk scores for vulnerabilities.	
		- Threat Intelligence Integration	Incorporates threat intelligence data into risk assessments.	
		- Business Impact Analysis	Assesses the potential impact of vulnerabilities on business operations.	
		Remediation Workflow Automation		
		- Workflow Automation	Automates the remediation process for identified vulnerabilities.	
		- Customizable Remediation Workflows	Defines and customizes workflows based on organizational needs.	
		Reporting and Analytics		
		- Vulnerability Reports	Generates reports on identified vulnerabilities and their status.	
		- Executive Dashboards	Provides high-level views for executives and management.	
		- Trend Analysis	Analyzes trends in vulnerability data over time.	
		Alerts and Notifications		
		- Real-time Alerts	Notifies administrators of critical vulnerabilities in real-time.	
		- Notification Preferences	Allows customization of notification methods and preferences.	
		Compliance and Audit Support		
		- Compliance Checks	Ensures that assets adhere to security and compliance standards.	
		- Audit Trails	Generates detailed logs for compliance audits.	
		Integration with Security Systems		

		- SIEM Integration	Shares vulnerability data with Security Information and Event Management systems.	
		- Integration with ITSM Systems	Integrates with IT Service Management tools for seamless collaboration.	
		Scanning Flexibility		
		- Authenticated Scanning	Conducts scans with authenticated access for deeper assessment.	
		- Unauthenticated Scanning	Performs scans without requiring user credentials.	
		Cloud Environment Support		
		- Cloud-Based Vulnerability Management	Manages vulnerabilities in cloud environments.	
		- Hybrid Cloud Support	Supports both on-premises and cloud-based vulnerability management.	
		Role-Based Access Control (RBAC)		
		- Delegation of Vulnerability Management Tasks	Allows delegation of tasks based on roles and responsibilities.	
		Scalability and Performance		
		- Scalability Support	Scales to accommodate the size and complexity of the IT environment.	
		- Minimal Performance Impact	Minimizes impact on assets and networks during scanning and remediation.	
10	Data Loss Prevention (DLP)	Prevention of Data Transfer	Providing the ability to prevent the transfer of data containing confidential information via SMTP, HTTP, HTTPS, FTP outside the corporate network;	
		Prevention of Data Transfer via Removable Media	Ensuring the possibility of preventing the se nding / recording of data containing confide ntial information on removable media (USB, SD / CF cards, CD / DVD), aswell as throu gh (WiFi, Bluetooth, etc.) interfaces;	

		Prevention of Printing	Provide the ability to prevent the printing of data containing confidential information on local and network printers;	
		Prevention of Unauthorized Operations	Ensuring the ability to prevent operations with data containing confidential information in PDF / Image, including screenshots (if it is impossible to provide - specify);	
		Prevention of Data Transfer to Network Directories	Ensuring the ability to prevent the transfer of data containing confidential information to network directories;	
		Scanning and detection	Providing the ability to scan file servers, databases, document management programs and user workstations for the presence of unauthorized storage locations of confidential information;	
		Automated remediation	Providing the ability to automatically move files containing confidential information from unauthorized storage locations of confidential information to a protected area;	
		Shadow copying	Providing the possibility of shadow copying of data containing confidential information;	
		Encryption	Ensuring the ability to encrypt data containing confidential information when copied to external media (if it is impossible to provide - specify);	
			Providing the ability to work both with labels and with the context of data containing confidential information;	
		Incident notification and management	Providing the ability to promptly notify security officers about incidents, both through the control console and alternative channels (mail, SMS, etc.), as well as the availability of mechanisms for investigating and processing incidents;	
		Reporting	Availability of a reporting subsystem;	
		Central Console	Providing the ability to manage through a single central console with web-based interface support;	

		MS Windows support	Providing the ability to prevent / monitor the transfer of data containing confidential information under MS Windows;	
		Perimeter control	The ability to control the following perimeter: transferring files from the local computer to File Share. Block or log security violations in thi s case.	
		Data Classification	The solution must have its own data classification module.	
		File transfer Monitoring	File transfer to removable media should be monitored by the number of files transferred or by the amount of information in Mb.	
		Security violation identification	The solution should provide the following functionality. Show which security violations are in the source file using the context menu.	
		Real time OCR	The solution must have real-time OCR functionality.	
		Watermarks	The solution should provide the ability to put water marks/print on: Computer screen, printed file, Microsoft office files and Microsoft Outlook letters.	
		Clipboard Control	The system must control the clipboard not only at the level of the copied text, but also the entire Microsoft office files copy.	
		Sceen Sharing	System must block screen Sharing when opening classified file.	
		File Share ID & Action	The system should execute the File Share ID and show the following actions: deleting a file, naming a file, creating a file.	
		Classification	The system must classify not only files but also classify at the folders.	
		Ad-hoc Classification	The system must provide ad-hoc classification.	
		OCR control	The presence of the OCR module to prevent copying to external media and data loss via the Internet on the endpoint agent.	

		Agent Support	There is an agent of endpoints for Ubuntu and Centos7, the presence of not only the detection function, but also the prevention of copying to external media, blocking the use of external media.	
		API Integration	System should have direct API to cloud storages.	
11	Packet Capture (PCAP) & Network Detection	Application Identification	The proposed solution must support out-of-the-box 3300+ application identification capabilities and share the list of the applications that can be identified.	
			The proposed solution must able to reconstruct email file attachments to support malware analysis and data loss monitoring.	
			The proposed solution must identify applications at Layer 7	
		Search and Filtering	The proposed solution must support structured search, unstructured search within the same query	
			The proposed solution must be based on Elastic Search Technology for fast and quick searching capability	
			The proposed solution must support search and live data filtering on both structured and unstructured network forensic data	
			The proposed solution should filter network traffic by individual devices	
			The proposed solution must support the ability to create basic &/or complex queries on network application data.	
			The proposed solution should perform searches across all network data	
			The proposed solution should be able to search attachment file names	

			The proposed solution shouldn't limit its alarms and searches by the size of the deployment or other restraints, for instance by the # of available CPU cores.	
		Packet Capture	The proposed solution must support full packet capture and smart capture. Smart Capture will automatically capture sessions based on application or packet content to drastically reduce your storage requirements while preserving the information you need.	
			The proposed solution must provide the ability to choose between capturing all packets and selective packet capture to lower storage requirements.	
			The Network Forensics must support GRE (Generic routing encapsulation) to deliver the network traffic to a remote Network Monitor for analysis without requiring a dedicated TAP or SPAN port	
		Network Behavior Analytics	The proposed solution must have a built-in Network Behavior Analytics engine for detecting abnormal network behavior	
			The proposed solution must detect and alert when inappropriate or blacklisted applications are used	

2. Cloud Hosting Services

In case of IT Security Services / Tools being provided using Cloud Hosted Services, the Supplier shall deploy such services / tools on a Ministry of Electronics and Information Technology (MeitY) empanelled Cloud Service Provider (CSP) including Data Centre (DC) and Disaster Recovery (DR) facility, with all necessary software components, databases and related applications and components, ensuring access and

availability of Information System to all concerned stakeholders and citizens. The provisioning of the Cloud Services should be strictly as per the guidelines of MeitY.

3. Operations and Maintenance

Overall Operations and Maintenance activities including IT Helpdesk services, for proposed Information System as per scope of this bid document, for entire project duration. This shall include operations and maintenance of the entire solution, Cloud services, Infrastructure, security services running on end devices, & networking services required to operate the IT Security Tools / Services and other support services. This may require the Supplier to deploy sufficient technical manpower required to provide services within the Service Level Agreements (SLAs) specified in the contract.

4. Training and Capacity Building

Training and Capacity Building activities including training of users for effectively using the tools and equipment of the proposed information system.

The Service Provider shall provide professional training by OEM or its Certified Training partner to the identified BMC employees / team/s on the solution for features / service architecture, and functionality during and after implementation.

5. Documentation and Version Control

Manage and maintain version control for all documents/ reports/ deliverables as well as application suite and databases with adequate security measures and protocols.

Documentation should be comprehensive & include:

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

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

6. Pre-Implementation Scope

6.1. Inception Report
6.2. Project Implementation Plan
6.3. System Design Documents
6.4. Requirement Traceability Matrix
6.5. Resource Deployment Plan
6.6. UAT / Testing Plan
5.7. Training Plan
5.8. Exit Management Plan

7. Implementation Scope

4.1 Project Implementation Plan

The success of the project depends on the proper project planning and management. At the onset, the MSP shall plan the project implementation in great details and should provide a micro level view of the tasks and activities required to be undertaken in consultation with

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

- Project Schedule: A detailed week-wise timeline indicating various activities to be performed along with completion dates and resources required for the same,
- Manpower Deployment List: A list needs to be provided with resources that will be deployed on the project along with the roles and responsibilities of each resource.
- Communication Plan: Detailed communication plan indicating what form of communication will be utilized for what kinds of meeting along with recipients and frequency.
- Progress Monitoring Plan and Reporting Plan: Detailed Daily, Weekly, Monthly Progress Report formats along with issue escalation format. The format will be approved by BMC to the successful bidder before start of the project.
- Standard Operating Procedures: Detailed procedures for operating and monitoring the Cloud site, Cloud management portal, etc.
- Risk Mitigation Plan: List of all possible risks and methods to mitigate them.
- Escalation Matrix & Incident Management: A detailed list of key contact persons with contact details with escalation hierarchy for resolution of issues and problems. This has to be via an Incident Management system.

6.5 Readiness and Risk Analysis

- Considering the criticality of the project to BMC, the service provider should study and submit a report of challenges envisaged from both organizational readiness standpoint, application readiness standpoint, integration standpoint (with existing infrastructure) and a risk standpoint.
- Successfully identifying and mitigating both technical and organization risks are a critical factor for setting up DC and disaster recovery site.
- Creating a comprehensive risk mitigation strategy outlining both preventative and compensatory actions will be necessary.

8. Post Implementation Scope

1. Ongoing Support and Maintenance

1.1. Establish a support mechanism for users to report issues and seek assistance.

1.2. Monitor system performance, identify, and resolve technical issues.

1.3. Conduct periodic system audits and performance assessments.

2. Evaluation and Continuous Improvement

2.1. Evaluate the system's effectiveness in meeting project objectives.

2.2. Collect feedback from users and stakeholders for system improvements.

2.3. Identify areas for enhancement and future upgrades.

2.4. Develop a plan for ongoing system enhancements and upgrades.

2.5. (a) Warranty Defect Repair and Technical Support Service Sub-Plan

C. Legal, Functional, Architectural, System Administration, Performance & Security Requirements

1. Legal and Regulatory Requirements to be met by the Information System

When designing and implementing Information System it is crucial to consider the legal and statutory requirements that govern the collection, storage, and processing data. The Supplier shall ensure following common legal and statutory requirements for Information System:

1.1 Data Protection and Privacy Laws:

- Comply with applicable data protection and privacy laws like DPDPA 2023.
- Implement appropriate security measures to protect personal and sensitive information stored in the Information System.
- Obtain necessary consent from individuals for the collection, storage, and processing of their personal data.

1.2 Security Safeguards: Implement robust security measures to protect data from unauthorized access, use, or disclosure. This includes technical and organizational safeguards such as access controls, encryption, authentication mechanisms, audit trails, and incident response procedures.

1.3 Records Management:

- Adhere to recordkeeping requirements imposed by legal, industry, or government regulations.
- Define document retention periods and disposal policies in compliance with relevant laws and regulations.
- Implement appropriate controls to ensure the integrity and authenticity of electronic records stored in the Information System.

1.4 Record Retention and Data Destruction: Comply with regulations regarding the retention and disposal of records.

1.5 Interoperability Standards: Ensure compliance with interoperability standards and regulations to facilitate the exchange of information with other providers, systems.

1.6 Intellectual Property Rights:

- Ensure compliance with copyright laws and respect intellectual property rights when storing and managing copyrighted documents or content within the Information System.
- Establish policies and procedures to prevent unauthorized sharing, distribution, or use of copyrighted materials.

1.7 Electronic Signatures and Authentication:

- Implement mechanisms for secure electronic signatures and authentication of documents within the Information System, if required by applicable regulations.

1.8 Legal Hold and eDiscovery:

- Implement features or processes within the Information System to support legal holds, which require the preservation of documents relevant to ongoing or potential litigation or investigations.
- Ensure the ability to perform efficient searches and retrieval of documents during the eDiscovery process, if necessary.

1.9 Audit Trail and Logging:

- Maintain an audit trail of user activities, document access, and modifications within the Information System to support compliance, investigations, or audits.
- Implement appropriate logging mechanisms and retain logs in accordance with legal and regulatory requirements as specified by CERT-In.

1.10 Data Breach Notification:

- Establish procedures to detect, respond to, and notify relevant parties in the event of a data breach or unauthorized access to documents stored in the Information System, as required by applicable data breach notification laws.

1.11 Documentation and Policy Requirements:

- Develop and maintain policies, procedures, and documentation related to the management, use, and security of documents within the Information System.
- Regularly review and update these policies to align with changing legal and regulatory requirements.

2. Functional/Technical/Operational Requirements to be met by the Information System

The Supplier is required to fulfill the functional/operational requirements of proposed Information Systems as detailed under Section B Scope of Work Sr. No. 1 List of IT Security Services / Tools covered under the scope of work.

3. Architectural Requirements to be met by the Information System

The architectural requirements of Information System define the overall structure, components, and technologies that enable the system to fulfill its functional requirements. The Supplier is required to fulfill following key architectural requirements for the Information System:

3.1 Modularity and Scalability: The Information System should be designed in a modular manner, with separate components or modules for different functionalities. This allows for flexibility in adding or modifying specific modules as per the BMC's requirements. The system should also be scalable, capable of handling increasing data volumes and user loads without significant performance degradation.

3.2 Centralized Database: The Information System typically requires a centralized and secure database to store and manage data. The database should support efficient data storage and retrieval, enforce data integrity and consistency, and provide mechanisms for data backup and recovery.

3.3 Interoperability: The Information System should be designed to facilitate interoperability with other Information systems and external entities. This includes the ability to exchange data with other systems. Standardized protocols and data formats (e.g., XML, CSV etc.) should be implemented to enable seamless integration and data exchange.

3.4 Web-Based Interface: A web-based user interface is often desirable for an Information System, as it provides accessibility from various devices and locations without the need for specific client installations. The interface should be intuitive, user-friendly, and responsive, allowing users to efficiently navigate through the system and perform their tasks.

3.5 Security and Privacy: Robust security measures should be incorporated into the Information System architecture to safeguard transaction data and ensure compliance with privacy regulations. This includes mechanisms for user authentication, access controls, data encryption, audit trails, and protection against unauthorized access or data breaches.

3.6 Integration Middleware: An Information System often requires middleware components to facilitate data integration and exchange between different systems. Integration middleware acts as a bridge, enabling seamless communication and data flow between the Information System and external systems or modules within the Information System architecture. This may involve the use of application programming interfaces (APIs), message queuing systems, or service-oriented architecture (SOA) principles.

3.7 High Availability and Disaster Recovery: The Information System should be designed with high availability and disaster recovery capabilities to ensure continuous access to critical information. This may involve redundant hardware configurations, load balancing, fault tolerance mechanisms, and data backup strategies to mitigate the impact of hardware or software failures, natural disasters, or other disruptive events.

3.8 Analytics and Reporting Framework: The Information System architecture should include a framework for data analytics and reporting. This may involve components such as dedicated analytics modules to enable the generation of meaningful insights from the data collected by the system.

3.9 Mobile Compatibility: With the increasing use of mobile devices, the Information System architecture may need to support mobile compatibility. This includes the ability to access and interact with the system using mobile applications or responsive web design optimized for mobile devices.

3.10 Standards and Interoperability Compliance: The Information System architecture should adhere to industry standards and interoperability frameworks to ensure compatibility and seamless data exchange with other systems. Standards such as xml, csv etc. are commonly used in the data exchange.

4. Systems Administration and Management Functions Required to be met by the Information System

The Systems Administration and Management functions of Information System involve the ongoing monitoring, maintenance, and optimization of the system to ensure its smooth operation and effectiveness. These functions are crucial for managing the technical infrastructure, user support, system upgrades, and overall governance of the Information System. The Supplier MUST provide for following key Systems Administration and Management functions of the Information System:

4.1 System Configuration:

- Configuration options to customize and adapt the Information System to the organization's needs, such as defining metadata attributes, document types, workflows, and templates.
- Ability to configure system-wide settings, including security parameters, retention policies, document storage locations, and system behavior.

4.2 User and Role Management:

- Ability to create, manage, and delete user accounts within the Information System.
- Role-based access control to assign different levels of privileges and permissions to users based on their roles and responsibilities.
- User provisioning and deprovisioning processes to efficiently manage user access.

4.3 Security and Access Control:

- Centralized management of security features, including user authentication and authorization mechanisms.
- Ability to define and manage user roles, permissions, and access rights.
- Integration with existing authentication systems, such as LDAP or Active Directory, for seamless user management.

4.4 Data Management and Security:

- Ensure data integrity, accuracy, and privacy by implementing robust data management practices.
- Regularly backup and archive data to prevent loss or corruption.
- Implement security measures, such as user authentication, access controls, and encryption, to protect sensitive health information.
- Stay updated with security best practices and address vulnerabilities through regular security assessments and patch management.

4.5 Backup and Recovery:

- Ability to schedule and perform regular backups of the Information System data.
- Configurable backup options, such as full or incremental backups, and support for various backup media or cloud storage.
- Recovery mechanisms to restore the Information System to a previous state in case of data loss or system failure.

4.6 System Integration and APIs:

- Integrate APIs and develop integration capabilities to connect the Information System with other systems or third-party applications.
- Manage and configure integration settings, including authentication credentials, data mapping, and synchronization options.

4.7 System Monitoring and Performance Management:

- Monitor the Information System infrastructure, including hardware, servers, networks, and databases, to ensure optimal performance.
- Implement monitoring tools and processes to track system availability, response times, and resource utilization.
- Identify and address performance bottlenecks or issues to maintain system efficiency.
- Logging and auditing capabilities to record and track user actions, document access, modifications, and system events.
- Capacity planning to ensure the Information System infrastructure can accommodate future growth and increasing demands.

4.8 User Support and Training:

- Provide user support and help desk services to address technical issues, system usage queries, and troubleshooting.
- Conduct regular training sessions to educate users on system functionalities and updates.
- Develop user manuals, guides, and knowledge bases to assist users in utilizing the Information System effectively.

4.9 Reporting and Analytics:

- Reporting tools and features to generate predefined or custom reports on system usage, performance, or document-related metrics.
- Analytics capabilities to analyze and derive insights from the Information System data, such as user behavior, document trends, or system performance.

4.10 Change Management and Governance:

- Establish change management processes to control system changes and minimize disruptions.
- Conduct impact assessments and risk analysis for proposed system changes or upgrades.
- Define and enforce governance policies and procedures to ensure compliance with regulatory requirements, industry standards, and organizational guidelines.
- Establish a change control board or committee to review and approve system changes.

4.11 System Upgrades and Maintenance:

- Plan and implement system upgrades, including software updates, bug fixes, and feature enhancements.
- Perform routine maintenance tasks, such as system configuration, optimization, and database management.
- Coordinate with vendors teams for system patches, bug resolutions, or new feature implementations.
- Schedule and perform system maintenance tasks, such as database optimization, index rebuilding, or performance tuning.

4.12 System Evaluation and Continuous Improvement:

- Monitor and evaluate the performance and effectiveness of the Information System against defined objectives and metrics.
- Collect user feedback and conduct surveys to gather insights for system improvement.
- Identify areas for enhancement, prioritize system enhancement requests, and plan for future or upgrades.
- Stay updated with emerging technologies and industry trends to leverage innovations that can benefit the Information System.

5. Performance Requirements of the Information System

Performance requirements for Information System define the desired levels of system performance in terms of speed, responsiveness, scalability, and reliability. Meeting these requirements ensures that the Information System can effectively handle user demands and provide timely access to critical health information. The Supplier shall fulfill following key performance requirements for an Information System:

5.1 Availability: The Information System should be highly available, ensuring uninterrupted access to critical health information. It should minimize downtime due to system maintenance, upgrades, or unforeseen failures. Availability requirements are specified in Service Level Agreement table.

5.2 Response Time: The Information System should exhibit fast response times, ensuring that users experience minimal delays when interacting with the system. Response times should be optimized for various operations, such as searching transaction records, retrieving test results, generating reports, or processing transactions. Response time requirements are specified in Service Level Agreement table.

5.3 Throughput: The Information System should have the capability to handle a high volume of transactions and user requests concurrently. It should be designed to handle peak loads without significant performance degradation. Throughput requirements may be defined in terms of the number of transactions processed per unit of time.

5.4 Scalability: The Information System should be scalable to accommodate increasing data volumes, user loads, and system complexity. Scalability can be achieved through vertical scaling (increasing hardware resources) or horizontal scaling (adding more servers or instances). The system should be able to handle future growth and expansions without sacrificing performance.

5.5 Concurrency: The Information System should support multiple concurrent users accessing and updating data simultaneously. It should handle concurrent transactions without conflicts, ensuring data consistency and avoiding data corruption or data integrity issues.

5.6 Security Performance: The Information System should incorporate robust security measures without compromising system performance. This includes authentication and authorization mechanisms, data encryption, and secure communication protocols. Security measures should be implemented efficiently to prevent performance degradation. Response time requirements are specified in Service Level Agreement table.

5.7 Data Retrieval and Reporting: The Information System should provide fast and efficient data retrieval capabilities, enabling users to access transaction records, reports, and other relevant information quickly. Report generation, including statistical reports and data analytics, should be performed in a timely manner.

5.8 Data Import and Export: The Information System should support efficient and timely data import and export processes. It should handle large data imports, without causing significant delays or performance issues. Data exports for sharing with external systems or generating data backups should also be performed in a reasonable timeframe.

5.9 System Monitoring and Logging: The Information System should include mechanisms for system monitoring, performance tracking, and logging. It should provide insights into system usage, resource utilization, and performance bottlenecks. Monitoring and logging should be optimized to capture relevant information without causing excessive system overhead.

6. Security Requirements of the Information System

Security is a critical aspect of Information System across its entire lifecycle to protect sensitive information, ensure confidentiality, integrity, and availability of data, and prevent unauthorized access or breaches. The Supplier must follow, provide and implement fulfill following key security requirements for the Information System for each phase:

4.2 Design:

- Threat modeling: Identify potential threats and vulnerabilities specific to the system and its environment.
- Risk assessment: Evaluate the potential risks associated with the system and prioritize them based on their impact and likelihood.
- Security architecture: Design a secure architecture that incorporates appropriate security controls, such as access controls, encryption, and intrusion detection systems.
- Data classification: Classify data based on sensitivity and define security measures accordingly.
- Security policies: Develop and document security policies and procedures that outline acceptable system usage, access control, and incident response.

4.3 Configuration:

- Clearly Define Default Settings: Need to reduce the likelihood of errors and simplify the configuration process for users by Providing clear default values for configuration and document default settings.
- Validate Configuration Changes: Implement mechanisms to validate configuration changes before they are applied.

- Secure Configuration Storage: Protect sensitive configuration information from unauthorized access, modification, or disclosure by using encryption, access controls, and auditing.

- Monitor Configuration Changes: Track and log all configuration changes to identify unauthorized modifications, troubleshoot issues, and maintain accountability by using tools that can alert you to changes in configuration files and settings.

- Implement Configuration Drift Detection: Check for configuration drift, where settings deviate from the intended configuration using automated tools and minimize manual configuration. Use scripts or configuration management tools to automate deployment.

- Test Configuration Changes: Test all configuration changes in a non-production environment before deploying them to production to identify any potential issues or unintended consequences.

- Document Configuration: Maintain clear and comprehensive documentation of all configuration settings and include explanations of each setting, its purpose, default values, and potential implications.

4.4 Installation:

- Secure installation: Ensure that hardware and software components are installed securely, following best practices and secure configuration guidelines.
- Security updates: Apply necessary security patches and updates to address known vulnerabilities in the installed components.
- System hardening: Disable unnecessary services, remove default accounts, and enforce secure configurations for hardware and software.
- Physical Security: Implement physical security measures to protect the Information System infrastructure, such as data centers, servers, and networking equipment. This includes secure access controls, surveillance systems, backup power supply, and environmental controls (e.g., temperature, humidity).
- Malware Protection: Deploy up-to-date antivirus and anti-malware solutions to detect and prevent malicious software from infecting the Information System infrastructure, workstations, and servers. Regularly update antivirus signatures and perform system scans to detect and mitigate any potential threats.

4.5 Testing:

- Security testing: Conduct regular security testing, including vulnerability assessments, penetration testing, and security code reviews, to identify and remediate security vulnerabilities.
- Incident response testing: Test incident response plans and procedures to ensure an effective response to security incidents.

4.6 Commissioning:

- User access controls: Implement user authentication, authorization, and access management mechanisms.
- Security monitoring: Deploy tools for monitoring system logs and detecting potential security incidents.
- Incident response: Establish procedures for handling security incidents and responding to breaches. Establish an incident response plan and procedures to handle security incidents, breaches, or unauthorized access attempts. This includes defining roles and responsibilities, incident reporting mechanisms, and steps to mitigate the impact of security incidents.
- System backups: Regularly back up system data to ensure data availability and recovery in case of system compromises.

4.7 Deployment:

- Change management: Establish processes for managing changes to the system and ensure that security is considered during change implementation.
- User awareness training: Provide security awareness training to system users to educate them about security risks and best practices.
- Secure remote access: Implement secure remote access mechanisms for authorized personnel.
- Security audits: Conduct regular security audits to assess the effectiveness of security controls. Security Audit to be conducted by CERT-In empaneled agency at a frequency specified by CERT-In from time to time (which is twice a year at present) including compliance of the audit observations / vulnerabilities within the time limit specified by CERT-In.

4.8 Operations:

- User management: Implement strong user access controls, enforce password policies, and regularly review user privileges. This includes user authentication (e.g., passwords, multi-factor authentication), role-based access control (RBAC), and user privilege management.
- Audit Trail and Logging: Maintain an audit trail and comprehensive logging system to record all activities within the Information System. This includes user actions, system events, and access attempts. Log files should be securely stored and regularly reviewed to detect and investigate any suspicious or unauthorized activities.
- Secure Communication: Implement secure communication protocols, such as encrypted channels and virtual private networks (VPNs), to protect data transmitted between different components of the Information System, as well as external systems or networks.
- **Security awareness training:** Continuously train users to recognize and report security threats. Conduct regular security awareness training for Information System users, including employees, administrators, and other BMC staff. Educate them about security best practices, potential risks, and their roles and responsibilities in maintaining the security of the Information System and transaction data.
- **Continuous monitoring:** Monitor system logs, network traffic, and security events to detect and respond to security incidents.
- **Incident response:** Maintain incident response capabilities and improve processes based on lessons learned.
- **Backup and recovery:** Regularly perform backups and test data restoration procedures. Implement regular data backup procedures and disaster recovery plans to ensure data availability and business continuity in the event of system failures, natural disasters, or other emergencies.
- **Vendor management:** Apply security controls when engaging third-party vendors. Ensure that third-party vendors and partners involved in the Information System implementation or providing related services adhere to appropriate security measures. This includes conducting due diligence, defining security requirements in contracts, and regularly assessing their security practices.
- **Compliance and Regulatory Requirements:** Ensure compliance with relevant service regulations, data protection laws, and industry standards that govern the handling of transaction information and security practices.

4.9 Maintenance:

Vulnerability management: Regularly scan for vulnerabilities and apply necessary patches and updates to address them. Stay up to date with the latest software updates, patches, and security fixes provided by the Information System Supplier / Original Equipment Manufacturer (OEM). Implement a patch management process to address any identified security vulnerabilities.

- System updates: Keep software and firmware up to date to address security vulnerabilities.
- Configuration management: Maintain proper configuration of system components.
- Security incident response: Continuously improve incident response processes based on lessons learned.
- System retirement: Develop secure procedures for decommissioning and disposing of systems.

These security requirements help safeguard the information system and protect against potential threats and vulnerabilities. It is important to adapt and update security measures to address emerging threats and comply with applicable laws and regulations. Additionally, the Supplier should conduct regular security assessments and engage with security professionals to ensure a comprehensive and robust security posture throughout the system's lifecycle.

D. SERVICE SPECIFICATIONS – PROVISION TOOLS

7. System Analysis, Design and Configuration

System analysis, design, and configuration are crucial phases in the implementation of Information System. These phases involve gathering requirements, designing the system architecture, and configuration the software components. The Supplier shall fulfill following requirements for each phase:

System Analysis:

7.1 Requirement Gathering: Conduct interviews, surveys, and workshops with stakeholders to understand their needs and expectations. Identify functional requirements (e.g., user registration, appointment scheduling, billing), non-functional requirements (e.g., performance, security), and constraints (e.g., regulatory compliance).

7.2 Stakeholder Analysis: Identify and analyze the different stakeholders involved in the Information System, such as administrators, employees, users, and external agencies. Understand their roles, responsibilities, and information needs within the system.

7.3 Workflow Analysis: Analyze existing workflows and processes within the department/s to identify areas for improvement and automation. Document the flow of information, interactions, and decision points between different stakeholders.

7.4 Data Analysis: Analyze the types of data required for the Information System. Define data structures, relationships, and data validation rules. Consider data privacy and security requirements.

System Design:

7.5 System Architecture: Design the overall system architecture, including hardware and software components, network infrastructure, and integration points with other systems. Consider scalability, fault tolerance, and performance requirements.

7.6 Database Design: Design the database schema, tables, and relationships to store and manage the Information System data. Consider data normalization, data integrity, and performance optimization. Incorporate security measures such as access controls and encryption.

7.7 System Integration: Identify interfaces and integration points with other existing systems within the department / organization. Define data exchange formats, communication protocols, and message standards.

7.8 Documentation to be delivered as part of System Analysis, Design and Configuration

7.8.1 Project Inception Report containing the following.

7.8.1.1 Project Implementation Plan: This document outlines the overall strategy, objectives, and activities for implementing the Information System project. It includes a timeline, milestones, resource allocation, and responsibilities. The implementation plan serves as a roadmap for the project team and stakeholders.

7.8.1.2 Communication Plan: The communication plan details how project communication will be managed throughout the implementation process. It includes information on communication channels, frequency, stakeholders, and the types of information to be communicated. The plan ensures effective communication among project team members, stakeholders, and users.

7.8.1.3 Risk Management Plan: The risk management plan identifies potential risks and outlines strategies for mitigating and managing them. It includes a risk register, risk assessment, and risk response

plans. The plan helps anticipate and address potential obstacles that may arise during the implementation of the Information System.

7.8.1.4 Training Plan: The training plan defines the approach for training end-users on how to use the Information System effectively. It includes training objectives, curriculum, delivery methods, schedules, and resources required for training. The plan ensures that end-users receive the necessary knowledge and skills to utilize the Information System.

7.8.1.5 Testing and Quality Assurance Plan: The testing and quality assurance plan defines the approach for testing the Information System for functionality, performance, and accuracy. It includes test objectives, test cases, test scripts, and acceptance criteria. The plan ensures that the Information System meets the defined requirements and quality standards before going live.

7.8.1.6 Change Management Plan: The change management plan addresses how changes and updates to the Information System will be managed during and after implementation. It includes change request processes, change control procedures, and change impact assessment. The plan helps minimize disruption and ensures that changes are implemented smoothly.

7.8.1.7 Go-Live Plan: The go-live plan outlines the activities, procedures, and timelines for transitioning from the configuration phase to the operational use of the Information System. It includes tasks such as system deployment, user training, data migration, and post-go-live support. The plan ensures a smooth and successful transition to the live environment.

8. System Integration (to other existing systems)

System integration is a crucial aspect of Information System as it enables seamless communication and data exchange between the Information System and other systems within the departments of the organization. The Supplier shall fulfill following common system integration requirements for an Information System:

8.1 Identity and Access Management Integration: Integrate the Information System with the organization's identity and access management system to ensure seamless user authentication, single sign-on, and user provisioning. This integration simplifies user management, enhances security, and improves user experience.

8.2 API and Integration Capabilities:

- Provide well-documented APIs (Application Programming Interfaces) that allow other systems or applications to access and interact with the Information System functionality.
- Support standard protocols and data formats, such as RESTful APIs, SOAP, XML, JSON, or OData, for seamless integration with different systems.
- Define authentication and authorization mechanisms for secure access to the Information System APIs and ensure proper data protection.

8.3 Email and Messaging Integration:

- Integrate with email clients or messaging systems to enable notifications, or task assignments through email or instant messaging.
- Support email attachments or links that directly access documents stored in the Information System, ensuring seamless document exchange and collaboration.

8.4 Integration with Enterprise Systems:

- Integrate with enterprise systems, such as Building Unique Identification System, Customer Relationship Management (CRM), Enterprise Resource Planning (ERP), or

Human Resources Management (HRM) systems (if required) etc., to enable Information System within the context of broader business processes.

- Other Applications, as and when requested by the department

8.5 Reporting and Analytics Integration:

- Provide integration capabilities with reporting or analytics platforms to extract and analyze document-related metrics, user activities, or system performance data.
- Enable data exchange between the Information System and these platforms to generate comprehensive reports or perform advanced analytics on Information System processes.

9. Training and Training Materials

Training is a critical component in the successful implementation and adoption of Information System. It ensures that users are equipped with the necessary knowledge and skills to effectively use the Information System. The Supplier shall provide following key training and training materials for the Information System:

9.1 User Training:

- Provide comprehensive training programs for end-users who will interact with the Information System on a regular basis.
- Cover fundamental concepts, features, and functionalities of the Information System, tailored to different user roles and responsibilities.
- Include hands-on exercises and practical examples to reinforce learning and application of Information System capabilities.

9.2 Administrator Training:

- Provide specialized training for system administrators or IT staff responsible for managing and maintaining the Information System infrastructure.
- Cover system configuration, installation, upgrades, and backup and recovery procedures.
- Train administrators on user and group management, access control settings, and security configurations within the Information System.
- Provide guidance on managing document types, metadata schemas, workflows, and retention policies.
- Train administrators on monitoring system performance, generating reports, and troubleshooting common issues.
- Address system customization options, including branding, interface configuration, and integration with other systems.

9.3 Documentation and Knowledge Base: Maintain a comprehensive documentation repository and knowledge base that includes training materials, FAQs, troubleshooting guides, and best practices. This serves as a reference for users to reinforce their learning and find answers to common questions.

9.4 User Support Channels: Establish user support channels, such as a helpdesk, online ticketing system, or dedicated support team, to address user queries, issues, and requests for assistance. Prompt and efficient support is crucial in ensuring user confidence and satisfaction with the Information System.

It's important to allocate adequate resources, including trainers, training facilities, and training technology, to ensure the successful delivery of training programs. The Supplier shall regularly assess the effectiveness of the training initiatives and make necessary adjustments to continuously improve

the user training experience. By addressing these training requirements, the Supplier can ensure that users and administrators have the necessary knowledge and skills to leverage the full potential of the Information System, resulting in increased productivity, improved Information System practices, and successful adoption of the system within the organization.

10. Documentation Requirements

Documentation is essential for the effective implementation, operation, and maintenance of Information System. The Supplier shall ensure that the following key documentation requirements are fulfilled for the Information System:

10.1 System Documentation: Create comprehensive documentation that describes the Information System system architecture, infrastructure requirements, hardware and software dependencies, and network configurations. This documentation provides an overview of the system and serves as a reference for system administrators and IT personnel.

10.2 User Manuals and Guides: Develop user manuals and guides that explain how to navigate and use the Information System. These documents should provide step-by-step instructions, screenshots, and examples to assist users in performing various tasks within the system. User manuals can cover different modules or functionalities of the Information System, tailored to specific user roles or departments.

10.3 Standard Operating Procedures (SOPs): Document the standard operating procedures that outline the recommended processes and workflows within the Information System. SOPs provide guidelines for tasks such as user registration, appointment scheduling, data entry, result reporting, and billing. They help ensure consistency, accuracy, and efficiency in the use of the Information System across the organization.

10.4 Data Dictionary: Prepare a data dictionary that defines the data elements, attributes, and their meanings within the Information System. This document provides a common understanding of the data used in the system and facilitates data entry, reporting, and analysis. The data dictionary should include definitions, data types, allowable values, and any specific business rules or constraints associated with each data element.

10.5 Reporting and Analytics Documentation: Document guidelines and instructions for generating reports and analyzing data within the Information System. This includes information on available report templates, report parameters, filters, and visualization options. The documentation should also cover data extraction methods, data export formats, and any custom reporting features or tools.

10.6 Configuration and Customization Documentation: Document the configuration settings and customization options available in the Information System. This includes instructions on how to modify system settings, user roles, access controls, and preferences. The documentation should also cover guidelines for implementing and maintaining any customizations or system enhancements.

10.7 Training Materials: As mentioned earlier, develop training materials such as training manuals, presentations, and e-learning modules. These materials should be documented and organized in a manner that supports the training programs for Information System users. They serve as a reference for trainees and can be used for future training sessions.

10.8 Change Management Documentation: Document any changes or updates made to the Information System, including new features, bug fixes, and system enhancements. This includes release notes, change logs, and version control documentation. Tracking and

documenting changes help ensure transparency, traceability, and facilitate system maintenance and troubleshooting.

10.9 Support and Troubleshooting Documentation: Create documentation that outlines common issues, errors, and their resolutions related to the Information System. This documentation can include FAQs, troubleshooting guides, and known issues with their workarounds. It helps support personnel to efficiently handle user queries, address issues, and provide timely assistance.

10.10 Disaster Recovery and Business Continuity Documentation: Develop documentation that outlines the disaster recovery and business continuity plans for the Information System. This includes procedures for data backup, system restoration, contingency measures, and the roles and responsibilities of personnel during emergencies. Documentation should also cover data security measures, backup schedules, and recovery point objectives (RPO) and recovery time objectives (RTO).

Regular update and maintenance of the documentation should reflect any changes or updates to the Information System. The Supplier shall ensure that the documentation is easily accessible to relevant stakeholders and kept in a secure and organized manner. Good documentation practices will help facilitate system understanding, user adoption, support activities, and system maintenance in the long run.

11. Requirements of the Supplier's Technical Team

When implementing Information System, engaging with the supplier's technical team is crucial for a successful deployment. The Supplier is required ensure fulfillment of following common requirements for the Supplier's technical team in relation to the Information System:

11.1 Technical Expertise: The Supplier's technical team should consist of skilled professionals with expertise in Information System implementation, configuration, and customization. They should possess a strong understanding of service workflows, data management, and information systems in a government department setting.

11.2 System Installation and Configuration: The technical team should have the knowledge and skills to install and configure the Information System software and hardware components. They should be able to set up the required databases, servers, networks, and interfaces based on the system requirements and specifications.

11.3 Customization and Integration: If customization or integration with other systems is required, the technical team should possess the necessary expertise. They should be able to understand the specific needs of the department/s and tailor the Information System accordingly. This may involve customizing forms, workflows, reports, or interfaces to align with the organization's requirements.

11.4 System Testing and Quality Assurance: The technical team should conduct rigorous testing of the Information System to ensure its functionality, reliability, and performance. This includes both unit testing and system integration testing to validate different modules, interfaces, and workflows. They should have a structured approach to identify and resolve any issues or defects found during testing.

11.5 Documentation: The technical team should provide comprehensive documentation related to the Information System and the applications' implementation, including system specifications, configurations, customizations, and integration details. This documentation is essential for reference, troubleshooting, and future system maintenance.

11.6 Collaboration and Communication: Effective collaboration and communication with the department/s' IT team and other stakeholders are essential. The Supplier's technical team should actively engage in regular meetings, status updates, and coordination to ensure alignment with the organization's goals and expectations.

11.7 Project Management: The Supplier's technical team should include project managers who can effectively plan, coordinate, and oversee the implementation process. They should have experience in managing similar projects, ensuring adherence to timelines, and addressing any project-related issues or risks.

11.8 Training and Support: The technical team should provide comprehensive training to end-users on the Information System functionalities, usage, and administration. They should be capable of delivering effective training sessions, addressing user questions, and providing ongoing support during and after the implementation process. This includes offering helpdesk services or a dedicated support channel for prompt assistance.

11.9 System Upgrades and Maintenance: The Supplier's technical team should be responsible for system upgrades, patches, and maintenance. They should ensure that the Information System and the applications remains up-to-date with the latest software versions, security updates, and bug fixes. The team should proactively monitor the system's performance, address any technical issues, and apply necessary upgrades or fixes when required.

E. TECHNOLOGY SPECIFICATIONS – SUPPLY & INSTALL ITEMS

12. General Technical Requirements

12.1 **Language Support**: All information technologies must provide support for the *English and Marathi.* Specifically, all display technologies and software must support the Unicode / ISO character set and perform sorting according to ***appropriate standard method***.

12.2**Date Format**: All functionality MUST properly display, calculate, and transmit date data, in 21st-Century date data (DDMMYYYY) format.

12.3 Platform Flexibility

12.3.1 Web-centric, multi-tier architecture shall be used

12.3.2 Open Standards and Interoperability shall be considered

12.3.3 Compliance to SOA, Microservices and Web-services

12.4 Interoperability

12.4.1 Usage of standard APIs

12.4.2 Service-oriented architecture (SOA) and micro-services

12.4.3 Support for multiple industry standard databases with ODBC, JDBC and Unicode compliance

12.5 Adherence to various standards

Applications shall comply with Guidelines for Indian Government Websites. The system shall adhere to applicable IT standards published by the Department of Electronics and Information Technology, Government of India (www.deity.gov.in) and other applicable standards as listed in the table and also State Service Delivery Gateway (SSDG) and Mobile Service Delivery Gateway (MSDG). The website shall be validated for HTML, CSS, Broken Links, accessibility, and mobile friendliness. The Implementation agency shall ensure that the Solution is based on and compliant with industry standards (their latest versions as on date) wherever applicable. This shall apply to all the aspects of solution including but not limited to design, configuration, security, installation, and testing. There are many

standards that are indicated throughout this report, as well as summarized below. However, the list below is just for reference and is not to be treated as exhaustive.

Area	Standard
Information access/ transfer protocols	SOAP, HTTP/HTTPS
Interoperability	Web Services, Open standards
Information Security	System to be ISO27001 compliant
Operational integrity and security management	System to be ISO17799 compliant
IT Infrastructure management	ITIL / EITM specifications
Service Management	ISO 20000 specifications
Project Documentation	IEEE/ISO specifications for documentation
Internet Protocol	IPv4 and IPv6 ready equipment
Information System Application	Web enabled application

12.6ISO 27001 certification

The implementation agency has to apply, obtain and maintain the ISO 27001 certification for the project. The cost incurred for obtaining and maintaining the certification shall be borne by the Supplier. The Information System project shall comply with ISO 27001 standards and the Supplier shall get the certificate within three quarters from the date of Operational Acceptance of Information System failing which the subsequent payments will be deferred till the certification is obtained.

13. Computing Hardware / Software Specifications

Cloud Hosting Requirements of Information System

13.1Legal requirements of cloud hosting for Information System

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

13.1.1 Data Protection and Privacy Laws:

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

13.1.2 Data Residency and Sovereignty:

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

13.1.3 Confidentiality and Non-Disclosure:

- Implementing confidentiality and non-disclosure agreements with the cloud-hosting provider to protect transaction information and prevent unauthorized disclosure.

13.1.4 Service Level Agreements (SLAs):

- Negotiating and including SLAs that clearly define the responsibilities, obligations, and liabilities of both the Information System provider and the cloud hosting provider.
- Ensuring that the SLAs address uptime, data availability, data backup and recovery, and disaster recovery procedures.

13.1.5 Contractual Agreements:

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

13.1.6 Audit and Compliance:

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

13.1.7 Intellectual Property Rights:

- Ensuring that the Information System provider's intellectual property rights, including software, applications, and databases, are protected and not infringed upon by the cloud hosting provider.

13.1.8 Incident Response and Notification:

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

13.1.9 Data Ownership and Control:

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

13.1.10 Data Retention and Destruction:

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

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

13.2Functional requirements of cloud hosting services for Information System

When considering cloud hosting services for Information System, there are several functional requirements that should be considered. These requirements focus on the capabilities and features needed

to effectively host and manage the Information System in the cloud. The Supplier shall fulfill following common functional requirements of cloud hosting services for Information System:

13.2.1 Scalability and Elasticity:

- The cloud hosting service should provide the ability to scale the Information System infrastructure up or down based on demand.
- It should support automatic resource provisioning and dynamic allocation of computing resources to accommodate varying workloads.

13.2.2 Reliability and Availability:

- The cloud hosting service should ensure high availability and uptime for the Information System, minimizing downtime and service interruptions.
- It should have redundant infrastructure and data centers to provide failover capabilities and disaster recovery.

13.2.3 Data Backup and Recovery:

- The cloud hosting service should offer robust data backup mechanisms to protect against data loss.
- It should provide regular and automated backups of Information System data and ensure quick and efficient data recovery in case of system failures or disasters.

13.2.4 Security and Compliance:

- The cloud hosting service should implement strong security measures to protect sensitive transaction data and ensure compliance with relevant regulations or data privacy / protection laws applicable in India. .
- It should offer features like encryption, access controls, intrusion detection, and prevention systems, and regular security audits.

13.2.5 Performance and Response Time:

- The cloud hosting service should provide reliable and consistent performance for the Information System, with low latency and fast response times.
- It should have robust network infrastructure and optimized data transfer mechanisms to ensure efficient data access and processing.

13.2.6 Monitoring and Analytics:

- The cloud hosting service should offer monitoring and analytics tools to track the performance and health of the Information System infrastructure.
- It should provide real-time monitoring of resource utilization, network traffic, and system metrics to identify potential issues and optimize performance.

13.2.7 Integration and Interoperability:

- The cloud hosting service should support seamless integration with other systems and applications within the Information System ecosystem.
- It should provide APIs, protocols, or integration frameworks to facilitate data exchange and interoperability with external systems.

13.2.8 Management and Administration:

- The cloud hosting service should offer a user-friendly management interface or control panel to administer and configure the Information System infrastructure.
- It should provide features for managing user access, permissions, and roles within the cloud environment.

13.2.9 Support and Customer Service:

- The cloud hosting service should provide responsive and knowledgeable customer support to address any technical issues or concerns.
- It should offer 24/7 support, escalation procedures, and a dedicated support team familiar with functionality of department and Information System requirements.

These functional requirements will ensure that the cloud hosting service can effectively meet the needs of hosting and managing an Information System, providing a reliable, scalable, secure, and performant environment for data and applications.

13.3 Architectural requirements of cloud hosting services for Information System

Architectural requirements of Cloud Hosting Services for Information System project

When considering the architectural requirements of cloud hosting services for an Information System project, several factors should be taken into account. The Supplier shall fulfill following key architectural requirements:

13.3.1 Scalability: The cloud hosting architecture should support scalability to accommodate the growing needs of the Information System project. It should allow for easy scaling up or down of resources based on demand to ensure optimal performance and cost-efficiency.

13.3.2 High Availability: The cloud hosting architecture should provide high availability to ensure uninterrupted access to the Information System system. It should include redundancy and failover mechanisms to minimize downtime and maintain system availability in the event of hardware or software failures.

13.3.3 Fault Tolerance: The architecture should be designed to be fault-tolerant, meaning that it can continue to function properly even if certain components or services fail. This may involve implementing redundant systems, load balancing, and automated failover mechanisms.

13.3.4 Security: Security is of utmost importance in an Information System project. The cloud hosting architecture should incorporate robust security measures to protect sensitive transaction data and ensure compliance with relevant regulations. This may include encryption, access controls, intrusion detection and prevention systems, and regular security audits.

13.3.5 Data Backup and Disaster Recovery: The architecture should include provisions for regular data backups and disaster recovery. This involves storing data in multiple geographically dispersed locations and implementing backup and recovery mechanisms to minimize data loss and facilitate quick system restoration in the event of a disaster.

13.3.6 Network Connectivity: The architecture should provide reliable and high-speed network connectivity to ensure efficient communication between the Information System system components and end-users. This may involve selecting appropriate network providers and implementing robust networking infrastructure.

13.3.7 Integration Capabilities: The cloud hosting architecture should support seamless integration with other systems and services. This allows for data exchange and interoperability between different components of the Information System ecosystem.

13.3.8 Monitoring and Performance Management: The architecture should include monitoring and performance management capabilities to track system performance, identify bottlenecks, and ensure optimal resource utilization. This may involve implementing monitoring tools, performance analytics, and automated alerts for proactive issue resolution.

13.3.9 Compliance and Regulatory Requirements: The architecture should facilitate compliance with relevant regulatory requirements, such as data privacy and security regulations. It should support features like data encryption, audit trails, and access controls to meet the specific compliance needs of the Information System project.

13.3.10 Cost Optimization: The architecture should consider cost optimization strategies to ensure efficient resource utilization and minimize operational costs. This may involve using cost-effective cloud service models, such as on-demand pricing, reserved instances, or spot instances.

13.4 System administration and management function requirements for cloud hosting services for Information System

When utilizing cloud hosting services for Information System, there are several system administration and management function requirements to consider. These requirements focus on the tasks and responsibilities necessary to effectively administer and manage the Information System in a cloud environment. The Supplier shall fulfill following common system administration and management function requirements for cloud hosting services for Information System:

13.4.1 System Monitoring and Performance Management:

- Continuous monitoring of the cloud infrastructure to ensure optimal performance and resource utilization.
- Tracking and analyzing system metrics, such as CPU usage, memory usage, network latency, and disk space, to identify performance bottlenecks and optimize system performance.
- Setting up alerts and notifications for critical system metrics to proactively address any issues.

13.4.2 Provisioning and Configuration Management:

- Efficient provisioning of virtual machines, storage resources, and other necessary infrastructure components for the Information System.
- Managing the configuration of the cloud environment, including network settings, security groups, and access controls.
- Automating the provisioning and configuration processes to ensure consistency and reduce manual effort.

13.4.3 Security and Compliance Management:

- Implementing and managing robust security measures, such as access controls, firewalls, intrusion detection systems, and encryption mechanisms, to protect the Information System data and infrastructure.
- Regularly updating and patching the system with the latest security patches and software updates.
- Conducting vulnerability assessments and penetration testing to identify and address security vulnerabilities.
- Ensuring compliance with relevant regulatory requirements, such as Digital Personal Data Protection (DPDP) Act 2023 and maintaining appropriate documentation.

13.4.4 Backup and Disaster Recovery Management:

- Developing and implementing backup and disaster recovery strategies for the Information System data and infrastructure.
- Configuring and scheduling regular backups of critical data, applications, and configurations.

- Testing and validating the backup and restore processes to ensure data integrity and availability in the event of a disaster or system failure.
- Maintaining off-site backups and implementing replication or mirroring mechanisms for data redundancy.

13.4.5 Incident and Problem Management:

- Establishing processes for handling and resolving incidents and problems related to the Information System and the cloud hosting environment.
- Logging and tracking incidents and problems, prioritizing them based on severity and impact, and ensuring timely resolution.
- Conducting root cause analysis for major incidents and implementing preventive measures to minimize their recurrence.

13.4.6 Change and Release Management:

- Planning and managing changes to the Information System and the cloud environment in a controlled manner.
- Performing impact assessments for proposed changes and coordinating with relevant stakeholders for approvals and scheduling.
- Implementing version control and change tracking mechanisms to ensure proper documentation and accountability for system changes.

13.4.7 User Access and Identity Management:

- Managing user access and authentication mechanisms for the Information System and the cloud environment.
- Configuring user roles, permissions, and access controls to enforce proper data security and privacy.
- Implementing strong authentication mechanisms, such as multi-factor authentication, to protect user accounts.

13.4.8 Reporting and Documentation:

- Generating regular reports and documentation related to system administration and management activities, such as system performance reports, incident reports, and compliance documentation.
- Maintaining up-to-date documentation of the cloud environment, including configurations, network diagrams, and system procedures.

These system administration and management function requirements ensure that the cloud hosting services for Information System are effectively managed and maintained, providing a secure, stable, and well-performing environment for data and applications.

13.5 Performance requirements of cloud hosting services for Information System

When considering performance requirements for cloud hosting services for Information System, it is important to ensure that the cloud infrastructure can deliver the necessary performance to support the system's needs. The Supplier shall fulfill following key performance requirements:

13.5.1 Response Time: The cloud hosting service should provide low response times to ensure a smooth user experience. The Information System should be responsive and provide quick access to data and functionalities.

13.5.2 Scalability: The cloud infrastructure should be capable of scaling resources to accommodate varying workloads. This allows the Information System to handle increased user traffic or data processing requirements without significant performance degradation.

13.5.3 Availability: The cloud hosting service should guarantee a high level of availability, minimizing downtime and ensuring the Information System is accessible to users whenever needed. This can be achieved through redundancy, fault-tolerant architectures, and effective disaster recovery mechanisms.

13.5.4 Network Performance: The cloud hosting service should provide robust network connectivity with high bandwidth and low latency. This ensures efficient data transfer between the Information System and its users or external systems.

13.5.5 Data Transfer Speed: The cloud infrastructure should support fast data transfer speeds, particularly when exchanging large volumes of data. This is essential for activities such as uploading and downloading transaction records, images, or other data.

13.5.6 Database Performance: If the Information System relies on a database system, the cloud hosting service should ensure optimal database performance. This includes efficient query execution, indexing strategies, and appropriate database configuration to handle concurrent access and large data volumes.

13.5.7 Load Balancing: The cloud infrastructure should have load balancing mechanisms to distribute the workload evenly across multiple servers or instances. This helps prevent resource bottlenecks and ensures optimal performance even during peak usage periods.

13.5.8 Monitoring and Performance Optimization: The cloud hosting service should provide monitoring tools and analytics to track system performance. This allows administrators to identify and address performance bottlenecks, optimize resource utilization, and fine-tune the Information System for optimal performance.

13.5.9 Storage Performance: If the Information System relies on cloud storage services, the performance of data storage and retrieval should meet the system's requirements. This includes fast access to transaction records, images, or other stored data.

13.5.10 Integration Performance: If the Information System integrates with external systems or APIs, the cloud hosting service should ensure efficient integration and data exchange. This includes reliable and fast communication with external systems to minimize delays and support real-time data synchronization.

It is important to collaborate closely with the cloud hosting service provider to understand their performance capabilities and discuss specific performance requirements for the Information System. Regular performance testing and monitoring can help identify any performance issues and allow for proactive optimization and fine-tuning of the system.

13.6 Security requirements of cloud hosting services for Information System

When considering the security requirements of cloud hosting services for Information System, it is crucial to prioritize the protection of sensitive data and ensure compliance with relevant regulations. The Supplier shall fulfill following key security requirements:

13.6.1 Data Encryption: The cloud hosting service should provide robust encryption mechanisms to protect data at rest and in transit. This includes encryption of data stored in databases or cloud storage, as well as encryption of data transmitted over networks.

13.6.2 Access Control: The cloud hosting service should offer strong access control mechanisms to ensure that only authorized individuals can access the Information System and its data. This includes user authentication, role-based access control (RBAC), and fine-grained permissions management.

13.6.3 Network Security: The cloud infrastructure should have secure network configurations, including firewalls, intrusion detection and prevention systems (IDS/IPS), and virtual private networks (VPNs). These measures help protect the Information System from unauthorized network access and mitigate the risk of network-based attacks.

13.6.4 Threat Detection and Prevention: The cloud hosting service should have robust security monitoring systems in place to detect and respond to security threats promptly. This includes real-time monitoring of system logs, network traffic analysis, and the use of security information and event management (SIEM) tools.

13.6.5 Vulnerability Management: The cloud hosting service should regularly assess the system for vulnerabilities and apply necessary security patches and updates. This includes conducting vulnerability scans, penetration testing, and implementing a formal patch management process.

13.6.6 Data Backup and Disaster Recovery: The cloud hosting service should offer reliable data backup and disaster recovery mechanisms to ensure data integrity and availability in the event of system failures or disasters. This includes regular backups, off-site storage, and well-defined recovery procedures.

13.6.7 Recovery Point Objective (RPO) and Recovery Time Objective (RTO)

- Recovery Point Objective (RPO): RPO refers to the maximum amount of data loss that is deemed acceptable during the recovery process. It defines the point in time to which data must be recovered in order to resume normal operations. For an Information System, the RPO determines how frequently data backups or replication should be performed. A smaller RPO indicates a lower tolerance for data loss, meaning that more frequent backups or real-time replication may be required to minimize data loss in case of a failure. For this Information System project the RPO required to be maintained is 15minutes.
- Recovery Time Objective (RTO): RTO is the maximum tolerable duration of time within which the Information System must be recovered and made operational after a system failure or disaster. It represents the target time for system recovery and resumption of normal operations. The RTO includes the time required for system diagnosis, data restoration, system repair, and any necessary testing or validation. Achieving a shorter RTO typically involves implementing robust backup and recovery processes, efficient system monitoring, and automated failover mechanisms. For this Information System project the RTO required to be maintained is 2 hours.

13.6.8 Regulatory Compliance: The cloud hosting service should comply with relevant regulatory requirements, such as local data protection laws. It should provide necessary safeguards and controls to protect user's privacy and ensure compliance with data protection regulations.

13.6.9 Security Incident Response: The cloud hosting service should have a well-defined incident response plan and procedures to handle security incidents effectively. This includes prompt incident detection, containment, investigation, and communication of security breaches or incidents to relevant stakeholders.

13.6.10 Physical Security: The cloud hosting service should have physical security measures in place to protect the data centers where the Information System is hosted. This includes access controls, video surveillance, environmental controls, and disaster-resistant infrastructure.

13.6.11 Security Auditing and Compliance Reporting: The cloud hosting service should provide regular security audits and compliance reporting to demonstrate adherence to security standards and regulations. This includes providing audit logs, security assessment reports, and other documentation as required.

It is essential to thoroughly evaluate the security capabilities and certifications of the cloud hosting service provider. Additionally, ensure that a formal agreement is established to clearly define the security responsibilities and obligations of both parties. Regular security assessments and audits can help validate

the security posture of the Information System and ensure ongoing compliance with security requirements.

13.7 Documentation requirements of cloud hosting services for Information System

When it comes to documentation requirements for cloud hosting services for Information System, it is important to have comprehensive documentation to ensure effective system management, security, and compliance. The Supplier shall fulfill following key documentation requirements:

13.7.1 System Architecture and Configuration: Document the overall system architecture of the cloud hosting environment, including details of servers, networking components, storage systems, and virtualization technologies. Capture the configuration settings and parameters that are specific to the Information System deployment, such as virtual machine configurations, load balancing settings, and network configurations.

13.7.2 Security Documentation: Document the security measures implemented within the cloud hosting environment, including access control mechanisms, encryption methods, and network security configurations. This should include details on user access policies, authentication mechanisms, firewall rules, intrusion detection systems, and any other security features or controls in place.

13.7.3 Data Management and Backup: Document the data management practices, including data backup and restoration procedures within the cloud hosting environment. This should cover details such as backup schedules, retention periods, backup storage locations, and procedures for data recovery in case of a disaster or data loss.

13.7.4 Disaster Recovery Plan: Document the disaster recovery plan for the Information System, outlining the steps and procedures to be followed in the event of a system failure or major disruption. This should include details on data replication, failover mechanisms, recovery time objectives (RTOs), and recovery point objectives (RPOs).

13.7.5 Compliance Documentation: Document the compliance measures and certifications relevant to the cloud hosting service and the Information System. This may include documentation related to regulatory compliance standards such as local data protection laws. Maintain copies of compliance certificates, audit reports, and any other relevant documentation.

13.7.6 Incident Response and Handling: Document the incident response plan for the Information System, outlining the steps to be followed in the event of a security breach or incident. This should cover incident detection, response, containment, investigation, and reporting procedures. Include contact details of relevant stakeholders and incident response team members.

13.7.7 Change Management: Document the change management processes and procedures related to the cloud hosting environment and the Information System. This should cover details on how changes to the system are requested, reviewed, approved, implemented, and tested. Include change request forms, change approval records, and change implementation plans.

13.7.8 User Manuals and Guides: Develop user manuals and guides specifically tailored to the Information System deployment in the cloud hosting environment. These should provide detailed instructions on how to access and use the system, along with any specific features or functionalities available.

13.7.9 Monitoring and Performance Documentation: Document the monitoring and performance management practices within the cloud hosting environment. This should include details on the monitoring tools used, performance metrics tracked, and any performance optimization strategies or recommendations.

13.7.10 Support and Contact Information: Maintain an up-to-date list of support contacts, including the cloud hosting service provider's support team and any third-party vendors or consultants involved in supporting the Information System. Include contact information, escalation procedures, and response time expectations.

Regularly review and update the documentation as the Information System evolves, and ensure that it remains accessible to relevant stakeholders. Effective documentation helps ensure smooth system management, troubleshooting, and compliance with applicable regulations and standards.

14. Network and Communications Specifications

14.1 Legal requirements of networking for Information System project

When implementing Information System project, there are several legal requirements related to networking that need to be considered to ensure compliance and protect sensitive data. The Supplier shall fulfill following key legal requirements for networking in an Information System project:

14.1.1 Data Privacy Laws: Comply with applicable data privacy laws and regulations, such as the Digital Personal Data Protection (DPDP) Act 2023. These laws govern the collection, storage, and processing of personal health information and impose strict requirements on data protection, access controls, and data breach notification.

14.1.2 Network Security: Implement appropriate security measures to protect the Information System network and data from unauthorized access, data breaches, or other security incidents. This includes using firewalls, intrusion detection and prevention systems, access controls, encryption, and regular security assessments.

14.1.3 Access Controls: Implement strong access controls to ensure that only authorized personnel have access to the Information System network and data. This includes unique user accounts, strong passwords, role-based access controls, and regular user access reviews.

14.1.4 Network Monitoring: Implement network monitoring and logging mechanisms to detect and respond to security incidents, unauthorized access attempts, or other network anomalies. Monitoring can help identify and mitigate potential security threats and ensure compliance with legal requirements.

14.1.5 Data Transmission Encryption: Use encryption technologies, such as Secure Sockets Layer (SSL) or Transport Layer Security (TLS), to secure the transmission of sensitive data over the network. This helps protect data from unauthorized interception or tampering during transmission.

14.1.6 Network Resilience and Redundancy: Implement network redundancy and failover mechanisms to ensure the availability and resilience of the Information System network. This may include redundant network connections, load balancing, backup systems, and disaster recovery plans.

14.1.7 Compliance with Telecommunications Laws: Comply with applicable telecommunications laws and regulations, such as those governing the use of wireless communication or telecommunication services. Ensure that any telecommunication services used in the Information System project comply with relevant laws and regulations.

14.1.8 Intellectual Property Rights: Ensure that the networking infrastructure and technologies used in the Information System project do not infringe upon any intellectual property rights of third parties. This includes using licensed software, adhering to copyright laws, and respecting intellectual property rights associated with networking technologies.

14.1.9 Network Documentation: Maintain proper documentation of the Information System network, including network diagrams, configurations, IP address management, and inventory of network devices. This documentation is essential for compliance, troubleshooting, and network management purposes.

14.1.10 Contractual Agreements: Ensure that any contractual agreements with network service providers or vendors include provisions for compliance with legal requirements, data protection, security controls, confidentiality, liability, and dispute resolution.

It is important to consult with legal experts who specialize in functional services and technology laws to ensure that the networking implementation in the Information System project complies with applicable legal requirements. Additionally, regularly review and update network security measures and policies to adapt to evolving threats and changes in regulations.

14.2 Functional requirements of networking and communication for Information System project

The functional requirements of networking and communication for an Information System project can vary depending on the specific needs and goals of the deparment/s. However, the Supplier shall fulfill following common functional requirements:

14.2.1 Network Infrastructure: The Information System project requires a robust and reliable network infrastructure to support seamless communication and data transfer between various components of the system. This includes the deployment of switches, routers, access points, and other networking equipment to establish a secure and high-performing network.

14.2.2 Network Connectivity: The Information System project needs to ensure stable and high-speed connectivity upto the BMC data centre. This includes establishing wired and wireless connections to enable communication between different departments, units, and devices within the facility.

14.2.3 Data Security: The network infrastructure must implement strong security measures to protect sensitive transaction information and prevent unauthorized access. This includes implementing firewalls, intrusion detection and prevention systems, virtual private networks (VPNs), and encryption mechanisms to safeguard data during transmission.

14.2.4 Interoperability: The networking and communication components of the Information System should support interoperability standards to enable seamless integration with other systems and external entities. This facilitates the exchange of data with other service providers or systems.

14.2.5 Scalability: The network infrastructure should be scalable to accommodate the growing needs of the user departments. As the Information System expands and more users and devices are added to the network, it should be able to handle the increased traffic and maintain optimal performance.

14.2.6 Quality of Service (QoS): The network should prioritize traffic based on the specific needs of the Information System. Critical data, such as real-time transaction monitoring or emergency communication, may require higher bandwidth and lower latency to ensure timely and reliable delivery.

14.2.7 Network Monitoring and Management: The Information System project should include tools and processes for monitoring and managing the network infrastructure. This enables proactive identification and resolution of network issues, performance optimization, and capacity planning.

14.2.8 Voice and Video Communication: The networking requirements should consider the need for voice and video communication within the department/s. This may involve implementing Voice over IP (VoIP) solutions, video conferencing capabilities, and ensuring sufficient network bandwidth to support real-time communication.

14.2.9 Mobile Connectivity: If the Information System includes mobile devices or supports mobile applications, the network infrastructure should provide reliable and secure connectivity for these devices. This may involve implementing wireless access points, mobile device management (MDM) solutions, and ensuring seamless roaming within the facility.

14.2.10 Disaster Recovery and Redundancy: The networking requirements should include provisions for disaster recovery and redundancy to ensure continuous operation of the Information System in case of network failures or disruptions. This may involve implementing backup network connections, redundant hardware, and failover mechanisms.

These functional requirements should be analyzed and customized based on the specific needs and constraints of the department/s implementing the Information System project. It is crucial to involve network specialists and IT professionals with expertise in network systems to design and implement a

robust networking and communication infrastructure that meets the functional requirements and aligns with industry best practices.

14.3 Architectural requirements of networking and communication for Information System project

The architectural requirements of networking and communication for an Information System project play a crucial role in ensuring a reliable, secure, and scalable infrastructure. The Supplier shall fulfill following key architectural requirements:

14.3.1 Network Topology: Determine the appropriate network topology for the Information System project, such as a star, ring, or mesh topology, based on the facility's size, layout, and connectivity needs. Consider factors such as scalability, ease of management, and fault tolerance when designing the network topology.

14.3.2 Network Segmentation: Implement network segmentation to divide the network into separate segments or VLANs (Virtual Local Area Networks) based on functional or security requirements. This helps isolate critical systems, such as transaction data storage and management, from non-sensitive areas of the network.

14.3.3 Redundancy and Resilience: Design the network architecture with redundancy and resilience in mind to minimize single points of failure and ensure continuous operation. Implement redundant network links, switches, and routers to provide backup paths in case of network failures.

14.3.4 Scalability: Consider the scalability requirements of the Information System project to accommodate the growing number of users, devices, and data traffic. Plan for future expansion by incorporating scalability features such as modular network switches, adjustable bandwidth capacities, and flexible addressing schemes.

14.3.5 Network Security: Incorporate robust security measures into the network architecture to protect sensitive transaction data and ensure compliance with applicable regulations. Implement firewalls, intrusion detection and prevention systems, access controls, and encryption protocols to secure the network infrastructure.

14.3.6 Quality of Service (QoS): Define and prioritize network traffic based on the specific requirements of the Information System. Assign appropriate levels of bandwidth, latency, and packet prioritization to ensure reliable and optimal performance for critical applications such as real-time system monitoring or video conferencing.

14.3.7 Network Monitoring and Management: Include mechanisms for monitoring and managing the network infrastructure to ensure its health, performance, and security. Implement network monitoring tools, centralized management systems, and logging mechanisms to detect and address network issues promptly.

14.3.8 Integration with External Systems: Plan for the integration of the Information System network with external systems. Ensure that the network architecture supports the necessary protocols, interfaces, and data exchange mechanisms required for seamless interoperability.

14.3.9 Wireless Network Design: If the Information System project includes wireless connectivity, design and deploy a secure and reliable wireless network infrastructure. Consider factors such as coverage, capacity, and interference mitigation techniques to provide consistent and robust wireless connectivity within the department/s.

14.3.10 Network Documentation: Maintain comprehensive documentation of the network architecture, including network diagrams, configurations, IP addressing schemes, and connectivity details. This documentation aids in troubleshooting, future expansion, and compliance with regulatory requirements.

It is important to involve experienced network architects or consultants with expertise in network systems to design and implement the networking and communication architecture for the Information System

project. They can ensure that the architectural requirements are met, align with industry best practices, and adhere to relevant standards and regulations.

14.4 System administration and management function requirements of networking and communication for Information System project

The system administration and management function requirements of networking and communication for an Information System project are crucial for ensuring the smooth operation, maintenance, and optimization of the network infrastructure. The Supplier shall fulfill following key requirements in this area:

14.4.1 Network Monitoring: Implement network monitoring tools and systems to continuously monitor the performance, availability, and security of the network infrastructure. This includes monitoring network devices, bandwidth utilization, network traffic, and security events to identify and address potential issues proactively.

14.4.2 Configuration Management: Establish robust configuration management practices to effectively manage network devices, including switches, routers, firewalls, and access points. This involves maintaining an inventory of network devices, documenting configurations, and implementing standardized configuration templates to ensure consistency and ease of management.

14.4.3 Network Troubleshooting and Support: Develop processes and procedures for troubleshooting network issues and providing timely support to address network-related problems. This includes establishing a help desk or support team to respond to network-related incidents, diagnosing and resolving connectivity issues, and escalating complex problems to specialized network engineers if needed.

14.4.4 Network Performance Optimization: Regularly assess and optimize network performance to ensure optimal operation of the Information System. This includes monitoring network traffic patterns, identifying and resolving performance bottlenecks, optimizing network configurations, and implementing Quality of Service (QoS) measures to prioritize critical applications and traffic.

14.4.5 Network Security Management: Implement comprehensive network security management practices to protect the Information System and sensitive transaction data from security threats. This involves regularly updating network security policies, monitoring for vulnerabilities and attacks, applying patches and updates to network devices, and maintaining robust access controls and authentication mechanisms.

14.4.6 Change Management: Establish change management processes to manage and control changes to the network infrastructure. This includes documenting and reviewing proposed changes, assessing their impact on the network, testing changes in a controlled environment, and implementing changes in a controlled and coordinated manner to minimize disruptions and maintain system stability.

14.4.7 Backup and Disaster Recovery: Implement backup and disaster recovery strategies for the network infrastructure to ensure business continuity in the event of network failures or disasters. This involves regularly backing up network device configurations, maintaining off-site backups, and developing recovery procedures to restore network services quickly and efficiently.

14.4.8 Capacity Planning: Perform regular capacity planning exercises to anticipate future network resource requirements and ensure that the network infrastructure can handle the expected growth in users, devices, and data traffic. This includes analyzing historical usage data, forecasting future demands, and making necessary adjustments to network capacity, such as upgrading hardware or adjusting bandwidth allocations.

14.4.9 Vendor Management: Manage relationships with network equipment vendors, service providers, and contractors to ensure effective support, maintenance, and collaboration. This includes establishing service level agreements (SLAs), coordinating equipment repairs or replacements,

and staying informed about new technologies and updates that may benefit the network infrastructure.

14.4.10 Documentation and Reporting: Maintain comprehensive documentation of network configurations, changes, troubleshooting procedures, and performance metrics. This documentation serves as a reference for system administrators, facilitates knowledge sharing, and supports compliance requirements and audits.

By incorporating these system administration and management function requirements into the Information System project, BMC department/s can effectively manage and maintain the networking and communication infrastructure, ensuring optimal performance, security, and reliability for the Information System system.

14.5 Performance requirements of networking and communication for Information System project

The performance requirements of networking and communication for an Information System project are critical to ensure efficient and reliable access to information. The Supplier shall fulfill following key performance requirements:

14.5.1 Bandwidth: Determine the required bandwidth capacity to support the expected data traffic within the Information System. Consider factors such as the number of users, types of data being transmitted (e.g., images, audio, video), and the desired responsiveness of the system. Ensure that the network infrastructure provides sufficient bandwidth to handle peak loads and minimize latency.

14.5.2 Latency: Define acceptable latency levels for real-time communication and data retrieval within the Information System. Minimize latency to ensure timely access to information, especially for critical applications such as telemedicine, real-time monitoring, or remote consultations. Low-latency connections are essential for delivering a seamless user experience and facilitating efficient workflows.

14.5.3 Reliability: The networking and communication infrastructure should provide high reliability to ensure uninterrupted access to the Information System. Implement redundancy and failover mechanisms to minimize downtime and mitigate the impact of network failures. This may involve redundant network links, backup power systems, and redundant network devices to ensure continuous operation.

14.5.4 Scalability: Plan for the scalability requirements of the Information System project to accommodate the growing number of users, devices, and data traffic. The network infrastructure should be scalable to handle increased demand without compromising performance. Consider the ability to add additional network resources, such as switches, routers, and access points, as needed to support the expanding Information System environment.

14.5.5 Quality of Service (QoS): Define and prioritize network traffic based on the specific requirements of the Information System. Allocate appropriate levels of bandwidth, latency, and packet prioritization to critical applications, such as real-time video conferencing, medical imaging, or data transfers. QoS mechanisms can ensure that high-priority traffic receives the necessary network resources and prioritization over less critical traffic.

14.5.6 Network Response Time: Define acceptable network response time for various Information System functions, such as retrieving transaction records, accessing test results, or generating reports. Minimize response time to enhance user productivity and satisfaction. This requires optimizing network configurations, reducing latency, and ensuring efficient data transfer across the network.

14.5.7 Security Performance: Ensure that the networking and communication infrastructure can handle the required security measures without compromising performance. This includes implementing firewalls, intrusion detection and prevention systems, and encryption protocols to protect sensitive

data. Performance considerations should include the overhead of security protocols and mechanisms.

14.5.8 Data Transfer Speed: Consider the speed of data transfers within the Information System, especially for large files such as medical images or bulk data uploads. The network infrastructure should support high-speed data transfers to enable efficient sharing and retrieval of transaction information and other relevant data.

14.5.9 Network Monitoring and Optimization: Implement network monitoring tools and performance optimization techniques to proactively identify and address network performance issues. Regularly monitor network traffic, analyze performance metrics, and optimize network configurations to maintain optimal performance levels.

14.5.10 Network Resilience: Design the networking and communication infrastructure to be resilient and capable of recovering quickly from network disruptions or failures. Implement fault-tolerant mechanisms, such as redundant links, network load balancing, and failover systems, to minimize the impact of network outages on the Information System performance.

By incorporating these performance requirements into the design and implementation of the networking and communication infrastructure, BMC department/s can ensure that the Information System operates efficiently, providing fast and reliable access to information for improved service delivery.

14.6 Security requirements of networking and communication for Information System project

The security requirements of networking and communication for an Information System project are critical to safeguard sensitive transaction data and protect the integrity, confidentiality, and availability of the information. The Supplier shall fulfill following key security requirements:

14.6.1 Access Control: Implement strong access control measures to ensure that only authorized individuals can access the Information System and related network resources. This includes user authentication mechanisms such as passwords, multi-factor authentication, and role-based access control (RBAC) to enforce appropriate access privileges based on user roles and responsibilities.

14.6.2 Encryption: Encrypt sensitive data transmitted over the network to protect it from unauthorized interception or disclosure. Use secure protocols, such as SSL/TLS, for encrypting data in transit. Additionally, ensure that data at rest, such as stored transaction records and backups, are also encrypted to provide an extra layer of protection.

14.6.3 Network Segmentation: Segment the network into secure zones or virtual LANs (VLANs) to isolate different types of traffic and restrict unauthorized access between network segments. This helps contain potential security breaches and limits lateral movement within the network.

14.6.4 Intrusion Detection and Prevention: Deploy intrusion detection and prevention systems (IDS/IPS) to monitor network traffic, detect and block suspicious or malicious activities. These systems can help identify and respond to potential threats, including network-based attacks, malware, and unauthorized access attempts.

14.6.5 Firewalls: Implement firewalls to enforce access control policies and protect the network from unauthorized access or malicious traffic. Configure firewalls to allow only necessary network traffic and block potential threats, such as unauthorized incoming connections or malicious outbound traffic.

14.6.6 Secure Remote Access: If remote access to the Information System is required, implement secure remote access mechanisms such as Virtual Private Network (VPN) solutions. Ensure that remote access connections are encrypted and require strong authentication to prevent unauthorized access to the Information System and the network.

14.6.7 Network Monitoring and Logging: Deploy network monitoring tools and establish comprehensive logging mechanisms to track network activity, identify security incidents, and facilitate forensic

analysis in case of security breaches. Regularly review and analyze network logs to detect and respond to security events promptly.

14.6.8 Security Patch Management: Regularly apply security patches and updates to network devices, including routers, switches, firewalls, and intrusion detection/prevention systems. Keep abreast of vendor security advisories and promptly apply patches to address known vulnerabilities and protect the network infrastructure.

14.6.9 Security Awareness and Training: Conduct regular security awareness and training programs for all personnel accessing the Information System. Educate users about security best practices, such as creating strong passwords, recognizing phishing attempts, and avoiding unauthorized disclosure of sensitive information.

14.6.10 Incident Response and Disaster Recovery: Develop and implement an incident response plan to effectively respond to security incidents and breaches. This includes defining roles and responsibilities, establishing communication channels, and outlining procedures for containing, investigating, and mitigating security incidents. Additionally, establish robust backup and disaster recovery mechanisms to ensure the availability and integrity of the Information System in the event of a security incident or disaster.

It is essential to work closely with cybersecurity professionals and follow industry best practices to ensure that the networking and communication infrastructure of the Information System project meets the necessary security requirements. Regular security assessments, penetration testing, and ongoing security monitoring should also be conducted to identify and address any vulnerabilities or risks.

14.7 Documentation requirements of networking and communication for Information System project

Documentation plays a crucial role in capturing the design, implementation, and management aspects of the networking and communication infrastructure for an Information System project. The Supplier shall fulfill following essential documentation requirements for networking and communication:

14.7.1 Network Design Documentation: Document the overall network design, including network topology, hardware components, and network addressing schemes. This documentation should provide a clear understanding of how the network is structured and interconnected.

14.7.2 Network Diagrams: Create network diagrams that visually represent the network infrastructure, including routers, switches, firewalls, access points, and their interconnections. These diagrams help in understanding the network layout, identifying potential bottlenecks, and troubleshooting network issues.

14.7.3 Network Configuration Documentation: Document the configuration details of network devices, including routers, switches, firewalls, and wireless access points. This includes information such as IP addresses, VLAN configurations, routing protocols, access control lists (ACLs), and security settings. This documentation helps in managing and maintaining network devices and ensures consistency across the network.

14.7.4 Network Security Policies and Procedures: Document the security policies and procedures related to networking and communication. This includes information on access control mechanisms, firewall rules, encryption protocols, remote access policies, and incident response procedures. These documents serve as a reference for implementing and enforcing security measures.

14.7.5 Network Service Level Agreements (SLAs): Document the agreed-upon service levels for network performance, availability, and response time. This includes metrics, targets, and responsibilities for monitoring and maintaining network performance. SLAs help in managing expectations and holding service providers accountable.

14.7.6 Network Inventory: Maintain an inventory of network equipment, including hardware models, serial numbers, firmware versions, and warranty information. This documentation helps in

tracking the lifecycle of network devices, managing support and maintenance contracts, and ensuring timely updates and replacements.

14.7.7 Network Monitoring and Management Documentation: Document the procedures and tools used for network monitoring and management. This includes details about network monitoring systems, alerting mechanisms, log management, and performance optimization strategies. This documentation assists in troubleshooting network issues, analyzing performance trends, and maintaining network health.

14.7.8 Network Incident and Change Management: Document procedures and processes for handling network incidents and implementing changes to the network infrastructure. This includes incident response plans, change control procedures, and documentation templates for recording incident details, change requests, and their outcomes. These documents promote consistency, traceability, and accountability in managing network incidents and changes.

14.7.9 Network Testing and Validation: Document the procedures and results of network testing and validation activities. This includes test plans, test cases, and test results for network performance, security, and scalability testing. These documents provide evidence of the network's compliance with defined requirements and standards.

14.7.10 Network Troubleshooting Guides: Develop troubleshooting guides or knowledge base articles that capture common network issues, their potential causes, and recommended resolution steps. These guides assist network administrators in diagnosing and resolving network problems efficiently.

It is important to maintain documentation in a central repository, ensure it is regularly updated, and make it easily accessible to relevant stakeholders. Proper documentation ensures knowledge transfer, facilitates troubleshooting and maintenance activities, and provides a valuable resource for future enhancements or upgrades to the networking and communication infrastructure of the Information System project.

15. Monitoring Tool Requirements for Information System

Monitoring tool requirements for the Information System project should include following monitoring capabilities for Information System software application, cloud hosting services, network and communication services and end devices:

15.1 Real-time Monitoring: The tool should provide real-time monitoring capabilities to track the performance and availability of critical components in the Information System infrastructure.

15.2 Health Monitoring: The tool should be able to monitor the health of servers, databases, networking devices, and other infrastructure components, alerting administrators of any issues or anomalies.

15.3 Resource Utilization Monitoring: It should be able to monitor resource utilization metrics such as CPU usage, memory usage, disk space, and network bandwidth to identify potential bottlenecks or capacity issues.

15.4 Application Performance Monitoring: The tool should provide insights into the performance of Information System applications, including response times, transaction volumes, and resource consumption, to ensure optimal performance.

15.5 Alerting and Notification: The monitoring tool should have robust alerting capabilities to notify administrators and stakeholders promptly when predefined thresholds or conditions are breached. Alerts can be sent via email, SMS, or other communication channels.

15.6 Dashboard and Reporting: A user-friendly dashboard and reporting feature should be available to visualize key performance indicators, generate reports, and analyze historical data for capacity planning and performance optimization.

15.7 Event Logging and Auditing: The tool should have the ability to log events and provide an audit trail of activities for troubleshooting, compliance, and security purposes.

15.8 Scalability: The monitoring tool should be scalable to handle the growing needs of the Information System project, accommodating an increasing number of monitored components and data points.

15.9 Integration Capabilities: It should be able to integrate with other systems and tools within the Information System ecosystem, such as ticketing systems, log management tools, and configuration management databases, to enable seamless data exchange and correlation.

15.10 Security and Access Control: The monitoring tool should have robust security features, including role-based access control, authentication, and encryption, to ensure the confidentiality and integrity of monitoring data.

15.11 Customization and Extensibility: The tool should allow customization and extensibility to meet the specific monitoring requirements of the Information System project, including the ability to create custom metrics, dashboards, and alerts.

15.12 Historical Data Storage: Sufficient storage capacity should be available to retain historical monitoring data for analysis, trend identification, and compliance purposes.

When selecting a monitoring tool for an Information System project, it is important to consider the specific needs and requirements of the project, the complexity of the infrastructure, and the scalability and flexibility of the tool to accommodate future growth and changes.

16. Standard Software Specifications

The standard software specifications of Information System can vary depending on the specific Information System solution chosen and the requirements of the BMC department/s. However, the Supplier is required to meet the following common software specifications that are typically included in an Information System:

16.1 Operating System: The Information System software may be designed to run on a specific operating system, such as Windows, Linux, or macOS. The Supplier will specify the supported operating systems and versions.

16.2 Database Management System (DBMS): The Information System may utilize a specific DBMS to store and manage the data. Commonly used DBMS options include Microsoft SQL Server, Oracle Database, MySQL, or PostgreSQL. The Supplier will provide the compatible DBMS and version requirements.

16.3 Web Browser Compatibility: The Information System may be accessed through a web-based interface, and therefore, it should be compatible with popular web browsers such as Google Chrome, Mozilla Firefox, Microsoft Edge, or Safari. The Supplier will specify the recommended browser versions.

16.4 Programming Language and Framework: The Information System software may be developed using specific programming languages and frameworks. Commonly used programming languages include Java, C#, or PHP, while frameworks like .NET, Spring, or Laravel may be employed. The Supplier will provide information on the programming language and framework in which Information System is / will be developed.

16.5 Application Servers: Depending on the Information System architecture, it may require an application server to host and execute the Information System software. Examples of application servers include Apache Tomcat, Microsoft IIS, or Nginx. The Supplier will specify and provide the application server and version for the Information System.

16.6 Integration and Interoperability: The Information System may support various integration options and protocols to communicate with external systems. Common integration technologies include xml, csv etc. The Supplier will provide details on the supported integration standards and specifications.

16.7 Reporting and Business Intelligence: The Information System may include reporting and business intelligence capabilities. It may leverage specific reporting tools or frameworks such as Crystal Reports, JasperReports, or Power BI. The Supplier will specify and provide the compatible reporting tools and versions.

16.8 Security and Encryption: The Information System software should incorporate security features such as user authentication, access controls, and data encryption to protect transaction information. It may utilize standard encryption algorithms and protocols such as SSL/TLS for secure communication. The Supplier will provide information on the security measures implemented in the Information System.

16.9 User Interface and User Experience: The Information System should have an intuitive and user-friendly interface to facilitate easy navigation and efficient workflow. It may employ specific user interface frameworks or design principles to enhance usability. The Supplier may provide guidelines or recommendations for optimal user experience.

16.10 Mobile Compatibility: With the increasing use of mobile devices, the Information System may offer mobile compatibility through dedicated mobile apps or responsive web design. The Supplier may provide information on the supported mobile platforms, such as iOS and Android.

F. TESTING AND QUALITY ASSURANCE REQUIREMENTS

17. Pre-commissioning Tests

Pre-commissioning tests for Information System are conducted to ensure that the system is properly installed, configured, and ready for operational use. These tests help identify any issues or discrepancies before the system goes live. The Supplier shall conduct following common pre-commissioning tests for the Information System in consultation with users wherever necessary:

17.1 Test Planning and Strategy:

- Develop a comprehensive test plan that outlines the testing approach, objectives, scope, and schedule.
- Identify the test environments and resources required for testing.
- Define the test strategy, including the types of testing to be performed (e.g., functional, performance, security) and the level of automation.

17.2 Installation and Configuration Test: Verify that the Information System software is installed correctly on the designated servers and workstations. Ensure that all necessary components and modules are installed, and that the system is properly configured as per the Supplier's guidelines.

17.3 System Functionality Test: Test the functionality of the Information System by performing various tasks and transactions that represent typical usage scenarios. This includes creating and managing transaction records, scheduling appointments, generating reports, and performing billing operations. Ensure that all core features and modules of the Information System are functioning as expected. Validate workflows, access controls, permission settings, and collaboration features.

17.4 Data Integrity Test: Validate the integrity of data entered into the Information System. This involves checking if data is accurately captured, stored, and retrieved without any loss or

corruption. Test data consistency across different modules and verify that data validation rules and constraints are properly enforced.

17.5 Interoperability Test: If the Information System needs to interface or integrate with other systems or devices, conduct interoperability tests to ensure seamless data exchange. Test the compatibility and functionality of interfaces with other relevant systems.

17.6 Compatibility Testing:

- Test the Information System across various operating systems, web browsers, and devices.
- Ensure compatibility with different versions and configurations of these platforms.
- Validate the Information System 's behavior in different environments (e.g., local network, cloud, mobile).

17.7 Usability Testing:

- Evaluate the user-friendliness and intuitiveness of the Information System interface.
- Test workflows, navigation, and Information System tasks from end-user perspectives.
- Gather feedback from users to identify areas for improvement and optimize the user experience.

17.8 Regression Testing:

- Perform regression testing to ensure that new feature additions or bug fixes do not negatively impact existing functionalities.
- Test critical functionalities and workflows to ensure they continue to work after updates or changes to the Information System.

17.9 Performance and Load Test: Assess the performance of the Information System under normal and peak load conditions. Measure response times for various operations and transactions to ensure acceptable performance levels. Conduct stress testing to determine the system's stability and scalability by simulating high user loads and heavy data processing.

17.10 Security and Access Control Test: Validate the security measures implemented in the Information System. Test user authentication and access control mechanisms to ensure that user permissions are properly enforced. Conduct penetration testing to identify vulnerabilities and assess the system's resilience against security threats.

17.11 Disaster Recovery Test: Test the Information System's disaster recovery mechanisms and backup/restore procedures. Simulate data loss or system failure scenarios to ensure that backups are available and can be successfully restored. Verify the system's ability to recover and resume normal operations in the event of a disaster.

17.12 User Acceptance Test (UAT): Involve end-users and key stakeholders in user acceptance testing. Have them perform their routine tasks using the Information System and provide feedback on the system's usability, functionality, and adherence to their requirements. Incorporate their suggestions and address any issues identified during UAT.

17.13 Bug Tracking and Issue Resolution:

- Establish a robust bug tracking system to document and track identified issues during testing.
- Prioritize and address bugs based on severity and impact on Information System functionality.
- Collaborate with developers and stakeholders to resolve identified issues.

17.14 Documentation Review: Ensure that all system documentation, including user manuals, installation guides, configuration instructions, and operational procedures, are reviewed and

validated. Verify that the documentation is up to date, comprehensive, and aligned with the deployed Information System version.

17.15 Training Verification: Validate that the training provided to system administrators, end-users, and support staff is effective and sufficient. Test the knowledge and skills of the trained personnel to ensure they can operate the Information System confidently and perform their assigned tasks effectively.

The Supplier shall allocate dedicated resources, time, and expertise for testing and quality assurance activities to ensure that the Information System meets the desired quality standards and user expectations. The testing process should be well-documented, and any issues or bugs should be tracked, reported, and resolved in a timely manner.

18. Operational Acceptance Tests

Operational Acceptance Testing (OAT) for Information System is conducted to ensure that the system is ready for operational use and meets the requirements of the BMC department/s. OAT focuses on validating the overall functionality, performance, and usability of the Information System in a production-like environment. The Supplier shall conduct the operational acceptance tests in the following key areas for the Information System:

18.1Test Environment:

- Set up a dedicated test environment that closely resembles the production environment where the Information System will be deployed.
- Configure hardware, software, and network components to mirror the production environment as closely as possible.

18.2 Test Scenarios and Use Cases:

- Define a set of realistic and representative test scenarios that cover the major operational processes and workflows of the Information System.
- Create use cases that reflect typical user interactions with the system, including document creation, editing, sharing, and retrieval.

18.3 System Functionality: Verify that all core functions and modules of the Information System are operational and performing as expected. Test various scenarios that reflect real-world workflows / processes, such as user registration, appointment scheduling, transaction records management, billing and invoicing.

18.4Workflow and Process Testing: Assess the system's ability to support the BMC department's specific workflows and processes. Test end-to-end processes that involve multiple users and departments to ensure seamless flow of information and effective collaboration. Validate that the Information System streamlines processes and enhances efficiency in the BMC department/s.

18.5Usability and User Experience: Evaluate the user interface of the Information System to ensure it is intuitive, user-friendly, and meets the needs of different user roles.

18.6Performance and Response Time: Measure the system's performance under realistic operational conditions. Conduct tests to validate response times for common tasks and operations, such as searching for transaction records, generating reports, or processing large volumes of data. Ensure that the Information System meets performance requirements and operates within acceptable timeframes.

18.7Data Accuracy and Integrity: Validate the accuracy and integrity of data stored and processed by the Information System. Test data entry, retrieval, and update processes to ensure information

is correctly captured, stored, and displayed. Verify that data validation rules and constraints are enforced consistently to maintain data integrity.

18.8 Security and Access Controls: Verify that the Information System has appropriate security measures in place to protect transaction data and ensure authorized access. Test user authentication, access controls, and permission settings to ensure that only authorized users can access sensitive information. Evaluate the system's compliance with relevant data privacy and security regulations.

18.9 Error Handling and Fault Tolerance: Assess how the Information System handles errors, exceptions, and system failures. Test scenarios that simulate various error conditions, such as network connectivity issues, database failures, or input validation errors. Verify that the system handles errors gracefully, provides meaningful error messages, and recovers from failures without data loss or corruption.

18.10 Integration and Interoperability: Validate the interoperability of the Information System with other systems and devices within the BMC department's environment. Test the system's ability to exchange data with other relevant systems. Verify that data is accurately shared, and interfaces function correctly.

18.11 Documentation Verification: Review and validate all system documentation, including user manuals, operational procedures, and configuration guides. Ensure that the documentation is complete, up to date, and aligned with the deployed version of the Information System. Verify that end-users can reference the documentation effectively for system usage and troubleshooting.

18.12 User Acceptance Testing (UAT): Involve end-users and key stakeholders in the testing process. Have them perform their routine tasks using the Information System and provide feedback on the system's performance, usability, and alignment with their requirements. Address any issues identified during UAT and incorporate user feedback to improve the system.

By conducting comprehensive Operational Acceptance Testing, organizations, BMC users can gain confidence in the readiness and suitability of the Information System for operational use. It helps the Supplier to identify any potential issues, gaps, or areas for improvement before the system is deployed in a production environment.

G. SERVICE SPECIFICATIONS – RECURRENT COST ITEMS

19. Warranty Defect Repair

Warranty defect repair for Information System refers to the process of addressing and rectifying any software or hardware defects that occur within the warranty period provided by the Supplier. During this period, the Supplier is responsible for resolving issues that are covered under the warranty terms. The Supplier shall adopt following general steps involved in warranty defect repair for the Information System:

19.1 Issue Identification: The BMC user identifies a defect or issue in the Information System software or hardware that is covered under the warranty. The issue can be reported by end-users, system administrators, or IT staff who have encountered a problem while using the Information System.

19.2 Issue Reporting: The identified issue is reported to the Supplier or their technical support team. The reporting process typically involves providing detailed information

about the problem, including error messages, steps to reproduce the issue, and any other relevant information that can help the Supplier understand and reproduce the defect.

19.3 Vendor Evaluation: The Supplier reviews the reported issue to determine whether it falls within the scope of the warranty. They may ask for additional information or request remote access to the Information System to further investigate the problem.

19.4 Issue Resolution: Once the Supplier confirms that the reported issue is covered under the warranty, they work to resolve the defect. This can involve software bug fixes, code modifications, configuration adjustments, or hardware repairs/replacements, depending on the nature of the issue. The Supplier may provide updates or patches to address the defect.

19.5 Testing and Verification: After the Supplier implements the fix or resolution, they typically conduct testing to ensure that the defect has been successfully addressed and the Information System is functioning correctly. This may involve running test cases, validating the fix against the reported issue, and conducting regression testing to ensure that the resolution has not introduced new problems.

19.6 Deployment of Fix: Once the resolution is validated, the Supplier provides instructions for applying the fix or update to the Information System environment. The BMC department or their IT staff of the Supplier follow the provided instructions to implement the fix, ensuring that it is correctly applied to all affected components of the Information System.

19.7 Confirmation of Resolution: The BMC user verifies that the defect has been resolved by retesting the affected functionality in the Information System. They ensure that the fix has successfully resolved the issue and that the system is functioning as expected.

19.8 Documentation and Closure: The Supplier shall maintain proper documentation of the defect, the resolution process, and any relevant communication related to the warranty defect repair. Once the defect is successfully resolved, the issue is considered closed, and both parties acknowledge the completion of the warranty repair process.

Communication and collaboration between the department staff and the Supplier's technical support team are vital throughout the warranty defect repair process to ensure timely and effective resolution of issues.

20. Technical Support

Technical support requirements for Information System involve the resources, services, and processes needed to assist users in resolving technical issues and maximizing the system's performance. The Supplier shall provide the following key technical support requirements for the Information System:

20.1 Help Desk: Establish a help desk or support center staffed with knowledgeable support personnel who can provide assistance to users. The help desk should be accessible through various channels, such as phone, email, live chat or a web-based ticketing system and dedicated support portal, to receive and track user requests for technical support. Adhere to the hours of operation for support services and any exceptions for after-hours or critical issue support, as specified in the contract.

20.2 Troubleshooting and Issue Resolution: The technical support team should have the expertise to troubleshoot and diagnose technical issues reported by users. They should be able to identify the root causes of problems and provide timely resolutions or workarounds. This may involve remote assistance, guidance on system configuration, software patches, or updates.

20.3 Knowledge Base and Documentation: Maintain a comprehensive knowledge base and documentation repository that contains troubleshooting guides, FAQs, user manuals, and other relevant resources. This enables support personnel to quickly access and share information to assist users in resolving common issues or answering frequently asked questions.

20.4 System Monitoring and Proactive Maintenance: Implement monitoring tools and processes to proactively monitor the performance, availability, and health of the Information System. This helps identify potential issues or system anomalies before they impact users. Regular maintenance activities, such as software updates, database optimizations, and hardware checks, should be performed to ensure the system's stability and performance.

20.5 Training and User Education: Offer training programs and resources to educate users on how to effectively use the Information System. This can include orientation sessions for new users, refresher training for existing users, and training on new features or updates. The technical support team should provide guidance on best practices, system usage, and workflows to help users maximize their productivity and minimize potential issues.

20.6 Escalation and Incident Management: Define escalation procedures and service level agreements (SLAs) for handling complex or critical technical issues. Establish clear communication channels and escalation paths to involve higher-level support or engage with the Supplier's technical experts, if necessary. Incident management processes should be in place to track, prioritize, and manage reported issues throughout their lifecycle.

20.7 System Upgrades and Migration Support: When system upgrades or migrations are required, the technical support team should provide assistance to ensure a smooth transition. This may involve validating system compatibility, performing data migration, coordinating downtime, and conducting post-upgrade testing to verify system functionality.

20.8 Vendor Collaboration and Coordination: Maintain a strong working relationship with the Information System / other support vendor's / OEM's technical support team. This includes regular communication, sharing of system logs or diagnostic information, and collaboration on resolving complex issues or identifying system improvements. The technical support team should act as a liaison between the department users and the Supplier to facilitate effective communication and issue resolution.

20.9 Continuous Improvement and Feedback Mechanisms: Implement feedback mechanisms, such as user satisfaction surveys or feedback loops, to gather input from users regarding the technical support services. Analyze user feedback to identify areas of improvement and implement necessary changes to enhance the support experience.

20.10 24/7 Support Availability: Depending on the BMC department's operational requirements, consider providing 24/7 technical support availability to ensure timely assistance and issue resolution, especially for critical or emergency situations.

The Supplier shall adhere to the service level agreements (SLAs) specified in the contract that outline the response times, resolution times, and support coverage for different types of technical issues. The technical support requirements should align with the BMC department's needs, budget, and the Supplier's support capabilities to ensure effective and efficient support services.

21. Requirements of the Supplier's Technical Team

21.1 The Supplier MUST provide a technical team to cover the BMC's anticipated Post-Operational Acceptance Technical Assistance Activities Requirements including obeying the Service Level

Agreements as specified in the contract so as to ensure smooth and interruption-free operations and management of Information System.

H. Implementation Schedule, Terms of Payment & SLAs

Following is the implementation schedule alongiwith target dates / timelines within which each milestone is required to be completed by the Supplier. However, the Supplier may discuss the plan with BMC and any changes required in the plan may be agreed and done mutually.

22. Implementation Schedule Table

22.1 Total Project Contract Period is 42 months

22.2 Completion Period for Provisioning/Supply, Installation, Testing, Commissioning (SITC) and Operational Acceptance is 6 months

22.3 For Operation and Maintenance (O&M) from the date of Operational Acceptance Date is 36 months.

The following tables covers consolidated information on Implementation Schedule, Terms of Payment, Service Level Agreements (during SITC phase), pre-requisites for payment and Liquidated Damages if milestone is not achieved on target date during SITC phase. Service Level Agreements during Operations & Maintenance (O&M) period are specified separately under clause – Service Level Agreements for Information System during Operations & Maintenance (O&M) phase.

Price Schedule / Bill of Quantities / Bill of Materials (**PLEASE DO NOT FILL IN COMMERCIAL DETAILS / RATES IN THE FOLLOWING TABLE** - To be filled in the format to be downloaded by the Supplier from eTendering system directly). Table below is only for reference purpose only.

Summary of Cost Components (Price Schedules / Bill of Materials & Quantities including terms of payment and SLAs for SITC phase)

Item No.	Name of the Tool	No. of License Quantity	Unit of Measurement	Unit Rate	Price	Payment MileStone 1 – Completion of OAT	Payment Milestone 2 – O&M Quarterly	Liquidated Damages on Milestone 1
1	Identity & Access Management	20,000	Users	Rate to be filled in eTendering System		80% of Quoted Price	20% equated in 12 quarterly payments	0.5% per week or part thereof for delay in OAT of individual item
2	Patch Management	20,000	Devices	Rate to be filled in		80% of Quoted Price	20% equated in 12	0.5% per week or part

				eTendering System			quarterly payments	thereof for delay in OAT of individual item
3	IT Asset Management	20,000	Devices	Rate to be filled in eTendering System		80% of Quoted Price	20% equated in 12 quarterly payments	0.5% per week or part thereof for delay in OAT of individual item
4	Network Access Control	20,000	Devices	Rate to be filled in eTendering System		80% of Quoted Price	20% equated in 12 quarterly payments	0.5% per week or part thereof for delay in OAT of individual item
5	Privilege Access Management	50	Users	Rate to be filled in eTendering System		80% of Quoted Price	20% equated in 12 quarterly payments	0.5% per week or part thereof for delay in OAT of individual item
6	Active Directory Management	17,000	Users	Rate to be filled in eTendering System		80% of Quoted Price	20% equated in 12 quarterly payments	0.5% per week or part thereof for delay in OAT of individual item
7	Vulnerability Management	20,000	Devices	Rate to be filled in eTendering System		80% of Quoted Price	20% equated in 12 quarterly payments	0.5% per week or part thereof for delay in OAT of individual item
8	Endpoint Detection and Response (EDR)	20,000	Devices	Rate to be filled in eTendering System		80% of Quoted Price	20% equated in 12 quarterly payments	0.5% per week or part thereof for delay in OAT of

								individual item
9	Application Performance Monitoring (APM)	150	Servers	Rate to be filled in eTendering System		80% of Quoted Price	20% equated in 12 quarterly payments	0.5% per week or part thereof for delay in OAT of individual item
10	DLP-Data Loss Prevention	20,000	Devices	Rate to be filled in eTendering System		80% of Quoted Price	20% equated in 12 quarterly payments	0.5% per week or part thereof for delay in OAT of individual item
11	Packet Capture & Network Detection (1 GBPS)	36	Months	Rate to be filled in eTendering System		80% of Quoted Price	20% equated in 12 quarterly payments	0.5% per week or part thereof for delay in OAT of individual item
12	Network connectivity (2 Lines of 1 Gbps each for a period of 36 months = Quantity 2 Lines x 36 months = 72 Lines-Months)	72	Lines-Month	Rate to be filled in eTendering System			Yearly Payment	0.5% per week or part thereof for delay in provisioning

Note: -

- Above Quantity is indicative. BMC reserves right to increase/decrease quantity up to 25% at the time of Purchase order.
- Payment as per actuals usage.
- Successful Operational Acceptance Test of each phase shall be considered partial Go-Live of the Information System Solution.
- Operations & Maintenance period will only start after successful OAT of all the Information System solution listed in the above table.

- Service Level Agreements (SLAs) and related liquidated damages on the items of work during Operations & Maintenance phase are given in the table below.

23. Service Level Agreements for Information System during Operations & Maintenance (O&M) Phase

A Service Level Agreement (SLA) for Information System outlines the agreed-upon levels of service and performance between the Supplier of Information System and the BMC. The Supplier shall fulfill following SLAs regarding system availability, response times, support, and other key metrics during O&M Phase of the project.

SR. No.	Service Category	SLA No.	Service Level Agreement	Breach Threshold calculated as	Liquidated Damages
23.1	Uptime of all solutions in the RFB	23.1.1	Measures the expected Uptime ad availability of all solutions in the RFB	System availability falling below 99.9% in a calendar month	The tools not meeting the criteria will attract 1% of quarterly contract price of O&M phase per every 0.1 % drop in the availability below the threshold for each tool. Each tools penalty will be calculated individually. Total penalty will be the sum of individual penalties.
23.2	Performance Metrics:	23.2.1	System Response Time: This measures the target response time for key operations such as record addition, retrieval, search, and upload.	Exceeding 5 seconds for average response time to user requests. This SLA will be measured randomly in a month in presence of the representative of the Supplier.	5% of quarterly contract price of O&M phase per incident of response time exceeding the threshold
23.3	Security and Data Protection of all solutions in the RFB	23.3.1	Data Security Measures: Describes resolution time to any security incidents	Exceeding 24 hours for resolution time to security incidents	5% of monthly contract price of O&M phase for each security vulnerability discovered and not remediated within timeframe specified by CERT-In which is immediate for Critical level, 24 hours for High level, 7 days for medium level and 30 days for Low level of severity
23.4	System Maintenance and Updates:	23.4.1	Maintenance Updates: This verifies that one version earlier than the latest patches released by Original	Non update of security patches of Operating System, Database and Other Software components upto 1	5% of quarterly contract price of O&M phase per week of delay in applying updates for each tool.

			Manufacturer of software are applied by the Supplier on Information System	level less than those released by Original Manufacturers of such software on quarterly basis	
23.5	Disaster Recovery and Business Continuity:	23.5.1	Recovery time objectives (RTO) and recovery point objectives (RPO).	RTO less than 2 hours or RPO less than 15 minutes	10% of quarterly contract price of O&M phase per hour of downtime exceeding RTO and 10% of quarterly contract price of O&M phase for data loss exceeding RPO or 20% of quarterly contract price if breach of both RTO and RPO is applicable
23.6	Support and Escalation:	23.6.1	Resolution Time: This measures the timeframe within which the Supplier resolves the requests or issues.	Exceeding 24 hours for fulfilment of support request or resolution of issues	INR 2000 per ticket per hour exceeding 24 hours
23.7	Reporting and Communication:	23.7.1	Performance Reports: This measures the frequency of submission of performance reports to be provided by the Supplier, including system availability, response times, and support statistics.	Non submission of reports on all SLAs listed in this section for every month on or before 5th of next month	5% of quarterly contract price of O&M phase per missed report

Section VI - General Conditions of Contract

A. CONTRACT AND INTERPRETATION

1. Definitions

a. In this Contract, the following terms shall be interpreted as indicated below.

i) contract elements

(1) "Contract" means the Contract Agreement entered into between BMC and the Supplier, together with the Contract Documents referred to therein. The Contract

Agreement and the Contract Documents shall constitute the Contract, and the term "the Contract" shall in all such documents be construed accordingly.

(2) "Contract Documents" means the documents specified in Article 1.1 (Contract Documents) of the Contract Agreement (including any amendments to these Documents).

(3) "Contract Agreement" means the agreement entered into between BMC and the Supplier using the form of Contract Agreement contained in the Sample Contractual Forms Section of the bidding documents and any modifications to this form agreed to by BMC and the Supplier. The date of the Contract Agreement shall be recorded in the signed form.

(4) "GCC" means the General Conditions of Contract.

(5) "SCC" means the Special Conditions of Contract.

(6) "Technical Requirements" means the Section - Technical Requirements in the bidding documents.

(7) "Implementation Schedule" means the Section - Implementation Schedule in the bidding documents.

(8) "Contract Price" means the price or prices defined in Article 2 (Contract Price and Terms of Payment) of the Contract Agreement.

(9) "Bidding documents" refers to the collection of documents issued by BMC to instruct and inform potential suppliers of the processes for bidding, selection of the winning bid, and Contract formation, as well as the contractual conditions governing the relationship between BMC and the Supplier. The General and Special Conditions of Contract, the Technical Requirements, and all other documents included in the bidding documents reflect the Procurement Regulations that BMC is obligated to follow during procurement and administration of this Contract.

ii) entities

(1) "Purchaser" means the entity purchasing the Information System / Services, which is Brihanmumbai Municipal Corporation (BMC).

(2) "Project Manager" means the person appointed by BMC in the manner provided in GCC Clause (Representatives - Project Manager) to perform the duties delegated by BMC.

(3) "Supplier" means the firm or Joint Venture whose bid to perform the Contract has been accepted by BMC and is named as such in the Contract Agreement.

(4) "Supplier's Representative" means any person nominated by the Supplier and named as such in the Contract Agreement or otherwise approved by BMC in the manner provided in GCC Clause (Representatives - Supplier's Representative) to perform the duties delegated by the Supplier.

(5) "Subcontractor" means any firm to whom any of the obligations of the Supplier, including preparation of any design or supply of any Information Technologies or other Goods or Services, is subcontracted directly or indirectly by the Supplier.

(6) "Adjudicator" means the person named in Appendix 2 of the Contract Agreement, appointed by agreement between BMC and the Supplier to make a decision on or to settle any dispute between BMC and the Supplier referred to him or her by the parties, pursuant to GCC Clause (Adjudication).

iii) scope

(1) "Information System," also called "the System," means all the Information Technologies, Materials, and other Goods to be supplied, installed, integrated, and made operational (exclusive of the Supplier's Equipment), together with the Services to be carried out by the Supplier under the Contract.

(2) "Subsystem" means any subset of the System identified as such in the Contract that may be supplied, installed, tested, and commissioned individually before Commissioning of the entire System.

(3) "Information Technologies" means all information processing and communications-related hardware, Software, supplies, and consumable items that the Supplier is required to supply and install under the Contract.

(4) "Goods" means all equipment, machinery, furnishings, Materials, and other tangible items that the Supplier is required to supply or supply and install under the Contract, including, without limitation, the Information Technologies and Materials, but excluding the Supplier's Equipment.

(5) "Services" means all technical, logistical, management, and any other Services to be provided by the Supplier under the Contract to supply, install, customize, integrate, and make operational the System. Such Services may include, but are not restricted to, activity management and quality assurance, design, development, customization, documentation, transportation, insurance, inspection, expediting, site preparation, installation, integration, training, data migration, Pre-commissioning, Commissioning, maintenance, and technical support.

(6) "The Project Plan" means the document to be developed by the Supplier and approved by BMC, pursuant to GCC Clause (Project Plan), based on the requirements of the Contract and the Preliminary Project Plan included in the Supplier's bid. The "Agreed Project Plan" is the version of the Project Plan approved by BMC, in accordance with GCC Clause (Project Plan). Should the Project Plan conflict with the Contract in any way, the relevant provisions of the Contract, including any amendments, shall prevail.

(7) "Software" means that part of the System which are instructions that cause information processing Subsystems to perform in a specific manner or execute specific operations.

(8) "System Software" means Software that provides the operating and management instructions for the underlying hardware and other components, and is identified as such in Appendix 4 of the Contract Agreement and such other Software as the parties may agree in writing to be Systems Software. Such System Software includes, but is not restricted to, micro-code embedded in hardware (i.e., "firmware"), operating systems, communications, system and network management, and utility software.

(9) "General-Purpose Software" means Software that supports general-purpose office and software development activities and is identified as such in Appendix 4 of the Contract Agreement and such other Software as the parties may agree in writing to be General- Purpose Software. Such General-Purpose Software may include, but is not restricted to, word processing, spreadsheet, generic database management, and application development software.

(10) "Application Software" means Software formulated to perform specific business or technical functions and interface with the business or technical users of the System and is identified as such in Appendix 4 of the Contract Agreement and such other Software as the parties may agree in writing to be Application Software.

(11) "Standard Software" means Software identified as such in Appendix 4 of the Contract Agreement and such other Software as the parties may agree in writing to be Standard Software.

(12) "Custom Software" means Software identified as such in Appendix 4 of the Contract Agreement and such other Software as the parties may agree in writing to be Custom Software.

(13) "Source Code" means the database structures, dictionaries, definitions, program source files, and any other symbolic representations necessary for the compilation, execution, and subsequent maintenance of the Software (typically, but not exclusively, required for Custom Software).

(14) "Materials" means all documentation in printed or printable form and all instructional and informational aides in any form (including audio, video, and text) and on any medium, provided to BMC under the Contract.

(15) "Standard Materials" means all Materials not specified as Custom Materials.

(16) "Custom Materials" means Materials developed by the Supplier at BMC's expense under the Contract and identified as such in Appendix 5 of the Contract Agreement and such other Materials as the parties may agree in writing to be Custom Materials. Custom Materials includes Materials created from Standard Materials.

(17) "Intellectual Property Rights" means any and all copyright, moral rights, trademark, patent, and other intellectual and proprietary rights, title and interests worldwide, whether vested, contingent, or future, including without limitation all economic rights and all exclusive rights to reproduce, fix, adapt, modify, translate, create derivative works from, extract or re-utilize data from, manufacture, introduce into circulation, publish, distribute, sell, license, sublicense, transfer, rent, lease, transmit or provide access electronically, broadcast, display, enter into computer memory, or otherwise use any portion or copy, in whole or in part, in any form, directly or indirectly, or to authorize or assign others to do so.

(18) "Supplier's Equipment" means all equipment, tools, apparatus, or things of every kind required in or for installation, completion and maintenance of the System that are to be provided by the Supplier, but excluding the Information Technologies, or other items forming part of the System.

iv) activities

(1) "Delivery" means the transfer of the Goods from the Supplier to BMC in accordance with the current edition Incoterms specified in the Contract.

(2) "Installation" means that the System or a Subsystem as specified in the Contract is ready for Commissioning as provided in GCC Clause (Installation of the System).

(3) "Pre-commissioning" means the testing, checking, and any other required activity that may be specified in the Technical Requirements that are to be carried out by the Supplier in preparation for Commissioning of the System as provided in GCC Clause (Installation of the System).

(4) "Commissioning" means operation of the System or any Subsystem by the Supplier following Installation, which operation is to be carried out by the Supplier as provided in GCC Clause (Commissioning and Operational Acceptance), for the purpose of carrying out Operational Acceptance Test(s).

(5) "Operational Acceptance Tests" means the tests specified in the Technical Requirements and Agreed Project Plan to be carried out to ascertain whether the System, or a specified Subsystem, is able to attain the functional and performance requirements specified in the Technical Requirements and Agreed Project Plan, in accordance with the provisions of GCC Clause (Commissioning and Operational Acceptance).

(6) "Operational Acceptance" means the acceptance by BMC of the System (or any Subsystem(s) where the Contract provides for acceptance of the System in parts), in accordance with GCC Clause (Commissioning and Operational Acceptance).

v) place and time

(1) "Supplier's Country" is the country in which the Supplier is legally organized, as named in the Contract Agreement.

(2) "Project Site(s)" means the place(s) in the Site Table in the Technical Requirements Section for the supply and installation of the System.

(3) "Day" means calendar day of the Gregorian Calendar.

(4) "Week" means seven (7) consecutive Days, beginning the day of the week i.e. Monday as is customary in India.

(5) "Month" means calendar month of the Gregorian Calendar.

(6) "Year" means twelve (12) consecutive Months.

(7) "Effective Date" means the date of fulfillment of all conditions specified in Article 3 (Effective Date for Determining Time for Achieving Operational Acceptance) of the Contract Agreement, for the purpose of determining the Delivery, Installation, and Operational Acceptance dates for the System or Subsystem(s).

(8) "Contract Period" is the time period during which this Contract governs the relations and obligations of BMC and Supplier in relation to the System, the Contract shall continue in force until the Information System and all the Services have been provided, unless the Contract is terminated earlier in accordance with the terms set out in the Contract.

(9) "Defect Liability Period" (also referred to as the "Warranty Period") means the period of validity of the warranties given by the Supplier commencing at date of the Operational Acceptance Certificate of the System or Subsystem(s), during which the Supplier is responsible for defects with respect to the System (or the relevant Subsystem[s]) as provided in GCC Clause (Defect Liability).

(10) "The Coverage Period" means the Days of the Week and the hours of those Days during which maintenance, operational, and/or technical support services (if any) must be available.

(11) "The Post-Warranty Services Period" means the number of years defined in the Section – BMC's Requirements (if any), following the expiration of the Warranty Period during which the Supplier may be obligated to provide Software licenses, maintenance, and/or technical support services for the System, either under this Contract or under separate contract(s).

2. Contract Documents

a. Subject to Article 1.2 (Order of Precedence) of the Contract Agreement, all documents forming part of the Contract (and all parts of these documents) are intended to be correlative, complementary, and mutually explanatory. The Contract shall be read as a whole.

3. Interpretation

a. Governing Language

i. All Contract Documents and related correspondence exchanged between BMC and Supplier shall be written in the language of these bidding documents (English), and the Contract shall be construed and interpreted in accordance with that language.

ii. If any of the Contract Documents or related correspondence are prepared in a language other than the governing language under GCC Clause above, the translation of such documents into the governing language shall prevail in matters of interpretation. The originating party, with respect to such documents shall bear the costs and risks of such translation.

b. Singular and Plural

The singular shall include the plural and the plural the singular, except where the context otherwise requires.

c. Headings

The headings and marginal notes in the GCC are included for ease of reference and shall neither constitute a part of the Contract nor affect its interpretation.

d. Persons

Words importing persons or parties shall include firms, corporations, and government entities.

e. Incoterms

Unless inconsistent with any provision of the Contract, the meaning of any trade term and the rights and obligations of parties thereunder shall be as prescribed by the Incoterms. Incoterms means international rules for interpreting trade terms published by the International Chamber of Commerce (latest edition), 38 Cours Albert 1er, 75008 Paris, France.

f. Entire Agreement

The Contract constitutes the entire agreement between BMC and Supplier with respect to the subject matter of Contract and supersedes all communications, negotiations, and agreements (whether written or oral) of parties with respect to the subject matter of the Contract made prior to the date of Contract.

g. Amendment

No amendment or other variation of the Contract shall be effective unless it is in writing, is dated, expressly refers to the Contract, and is signed by a duly authorized representative of each party to the Contract.

h. Independent Supplier

The Supplier shall be an independent contractor performing the Contract. The Contract does not create any agency, partnership, joint venture, or other joint relationship between the parties to the Contract. Subject to the provisions of the Contract, the Supplier shall be solely responsible for the manner in which the Contract is performed. All employees, representatives, or Subcontractors

engaged by the Supplier in connection with the performance of the Contract shall be under the complete control of the Supplier and shall not be deemed to be employees of BMC, and nothing contained in the Contract or in any subcontract awarded by the Supplier shall be construed to create any contractual relationship between any such employees, representatives, or Subcontractors and BMC.

i. Joint Venture
If the Supplier is a Joint Venture of two or more firms, all such firms shall be jointly and severally bound to BMC for the fulfillment of the provisions of the Contract and shall designate one of such firms to act as a leader with authority to bind the Joint Venture. The composition or constitution of the Joint Venture shall not be altered without the prior consent of BMC.

j. Nonwaiver
   i. Subject to GCC Clause below, no relaxation, forbearance, delay, or indulgence by either party in enforcing any of the terms and conditions of the Contract or the granting of time by either party to the other shall prejudice, affect, or restrict the rights of that party under the Contract, nor shall any waiver by either party of any breach of Contract operate as waiver of any subsequent or continuing breach of Contract.
   ii. Any waiver of a party's rights, powers, or remedies under the Contract must be in writing, must be dated and signed by an authorized representative of the party granting such waiver, and must specify the right and the extent to which it is being waived.
   iii. Severability If any provision or condition of the Contract is prohibited or rendered invalid or unenforceable, such prohibition, invalidity, or unenforceability shall not affect the validity or enforceability of any other provisions and conditions of the Contract.

k. Country of Origin

"Origin" means the place where the Information Technologies, Materials, and other Goods for the System were produced or from which the Services are supplied. Goods are produced when, through manufacturing, processing, Software development, or substantial and major assembly or integration of components, a commercially recognized product results that is substantially different in basic characteristics or in purpose or utility from its components. The Origin of Goods and Services is distinct from the nationality of the Supplier and may be different.

4. Notices

a. Unless otherwise stated in the Contract, all notices to be given under the Contract shall be in writing and shall be sent, pursuant to GCC Clause below, by personal delivery, airmail post, special courier, facsimile, electronic mail, or Electronic Data Interchange (EDI), with the following provisions.
   i. Any notice sent by facsimile, electronic mail, or EDI shall be confirmed within two (2) days after dispatch by notice sent by airmail post or special courier, except as otherwise specified in the Contract.
   ii. Any notice sent by airmail post or special courier shall be deemed (in the absence of evidence of earlier receipt) to have been delivered ten (10) days after dispatch. In proving the fact of dispatch, it shall be sufficient to show that the envelope containing such notice was properly addressed, stamped, and conveyed to the postal authorities or courier service for transmission by airmail or special courier.
   iii. Any notice delivered personally or sent by facsimile, electronic mail, or EDI shall be deemed to have been delivered on the date of its dispatch.
   iv. Either party may change its postal, facsimile, electronic mail, or EDI addresses for receipt of such notices by ten (10) days' notice to the other party in writing.

b. Notices shall be deemed to include any approvals, consents, instructions, orders, certificates, information and other communication to be given under the Contract.

c. Pursuant to GCC Clause (Representatives), notices from/to BMC are normally given by, or addressed to, the Project Manager, while notices from/to the Supplier are normally given by, or addressed to, the Supplier's Representative, or in its absence its deputy if any. If there is no appointed Project Manager or Supplier's Representative (or deputy), or for any other reason, BMC or Supplier may give and receive notices at their fallback addresses. The address of the Project Manager and the fallback address of BMC are as subsequently established/amended. The address of the Supplier's

Representative and the fallback address of the Supplier are as specified in Appendix 1 of the Contract Agreement or as subsequently established/amended.

5. Governing Law

a. The Contract shall be governed by and interpreted in accordance with the laws of India.

b. Throughout the execution of the Contract, the Supplier shall comply with the import of goods and services prohibitions in India when

i. as a matter of law or official regulations, India prohibits commercial relations with that country; or

ii. by an act of compliance with a decision of the United Nations Security Council taken under Chapter VII of the Charter of the United Nations, India prohibits any import of goods from that country or any payments to any country, person, or entity in that country.

6. Fraud and Corruption

a. BMC requires compliance with the BMC's Anti-Corruption Guidelines and its prevailing sanctions policies and procedures (as detailed in Section VI – Fraud and Corruption)

b. BMC requires the Supplier to disclose any commissions or fees that may have been paid or are to be paid to agents or any other party with respect to the bidding process or execution of the Contract. The information disclosed must include at least the name and address of the agent or other party, the amount and currency, and the purpose of the commission, gratuity or fee.

B. SUBJECT MATTER OF CONTRACT

7. Scope of the System

a. The Supplier's obligations cover the provision of all Information Technologies, Materials and other Goods as well as the performance of all Services required for the design, configuration, and implementation (including procurement, quality assurance, assembly, associated site preparation, Delivery, Pre-commissioning, Installation, Testing, and Commissioning) of the System, in accordance with the plans, procedures, specifications, drawings, codes, and any other documents specified in the Contract and the Agreed Project Plan.

b. The Supplier shall, unless specifically excluded in the Contract, perform all such work and / or supply all such items and Materials not specifically mentioned in the Contract but that can be reasonably inferred from the Contract as being required for attaining Operational Acceptance of the System as if such work and / or items and Materials were expressly mentioned in the Contract.

c. The Supplier's obligations (if any) to provide Goods and Services as implied by the Recurrent Cost tables of the Supplier's bid, such as consumables, spare parts, and technical services (e.g., maintenance, technical assistance, and operational support), are as specified in the Section – BMC's Requirements, including the relevant terms, characteristics, and timings.

8. Time for Commencement and Operational Acceptance

a. The Supplier shall commence work on the System within the period specified in the Implementation Schedule under Section – BMC's Requirements, and without prejudice to GCC Clause (Operational Acceptance Time Guarantee), the Supplier shall thereafter

proceed with the System in accordance with the time schedule specified in the Implementation Schedule and any refinements made in the Agreed Project Plan.

b. The Supplier shall achieve Operational Acceptance of the System (or Subsystem(s) where a separate time for Operational Acceptance of such Subsystem(s) is specified in the Contract) in accordance with the time schedule specified in the Implementation Schedule and any refinements made in the Agreed Project Plan, or within such extended time to which the Supplier shall be entitled under GCC Clause (Extension of Time for Achieving Operational Acceptance).

9. Supplier's Responsibilities

a. The Supplier shall conduct all activities with due care and diligence, in accordance with the Contract and with the skill and care expected of a competent provider of information technologies, information systems, support, maintenance, training, and other related services, or in accordance with best industry practices. In particular, the Supplier shall provide and employ only technical personnel who are skilled and experienced in their respective callings and supervisory staff who are competent to adequately supervise the work at hand.

b. The Supplier confirms that it has entered into this Contract on the basis of a proper examination of the data relating to the System provided by BMC and on the basis of information that the Supplier could have obtained from a visual inspection of the site (if access to the site was available) and of other data readily available to the Supplier relating to the System as at the date thirty (30) days prior to bid submission. The Supplier acknowledges that any failure to acquaint itself with all such data and information shall not relieve its responsibility for properly estimating the difficulty or cost of successfully performing the Contract.

c. The Supplier shall be responsible for timely provision of all resources, information, and decision making under its control that are necessary to reach a mutually Agreed Project Plan (pursuant to GCC Clause (Project Plan) within the time schedule specified in the Implementation Schedule. Failure to provide such resources, information, and decision-making may constitute grounds for termination pursuant to GCC Clause (Termination).

d. The Supplier shall acquire in its name all permits, approvals, and/or licenses from all local, state, or national government authorities or public service undertakings in India that are necessary for the performance of the Contract, including, without limitation, visas for the Supplier's and Subcontractor's personnel and entry permits for all imported Supplier's Equipment. The Supplier shall acquire all other permits, approvals, and/or licenses that are not the responsibility of BMC under GCC Clause (BMC's Responsibility) and that are necessary for the performance of the Contract.

e. The Supplier shall comply with all laws in force in India. The laws will include all national, provincial, municipal, or other laws that affect the performance of the Contract and are binding upon the Supplier. The Supplier shall indemnify and hold harmless BMC from and against any and all liabilities, damages, claims, fines, penalties, and expenses of whatever nature arising or resulting from the violation of such laws by the Supplier or its personnel, including the Subcontractors and their personnel, but without prejudice to GCC Clause (BMC's Responsibilities). The Supplier shall not indemnify BMC to the extent that such liability, damage, claims, fines, penalties, and expenses were caused or contributed to by a fault of BMC.

~~f.~~ The Supplier shall, in all dealings with its labor and the labor of its Subcontractors currently employed on or connected with the Contract, pay due regard to all recognized festivals, official holidays, religious or other customs, and all local laws and regulations pertaining to the employment of labor.

~~g.~~ Any Information Technologies or other Goods and Services that will be incorporated in or be required for the System and other supplies shall have their Origin, as defined in GCC Clause (Interpretation)

10. BMC's Responsibilities

a. BMC shall ensure the accuracy of all information and/or data to be supplied by BMC to the Supplier, except when otherwise expressly stated in the Contract.

b. BMC shall be responsible for timely provision of all resources, information, and decision making under its control that are necessary to reach an Agreed Project Plan (pursuant to GCC Clause (Project Plan)) within the time schedule specified in the Implementation Schedule. Failure to provide such resources, information, and decision making may constitute grounds for Termination pursuant to GCC Clause (Termination).

c. BMC shall be responsible for acquiring and providing legal and physical possession of the site and access to it, and for providing possession of and access to all other areas reasonably required for the proper execution of the Contract.

d. If requested by the Supplier, BMC shall use its best endeavors to assist the Supplier in obtaining in a timely and expeditious manner all permits, approvals, and/or licenses necessary for the execution of the Contract from all local, state, or national government authorities or public service undertakings that such authorities or undertakings require the Supplier or Subcontractors or the personnel of the Supplier or Subcontractors, as the case may be, to obtain.

e. In such cases where the responsibilities of specifying and acquiring or upgrading telecommunications and/or electric power services falls to the Supplier, as specified in the Technical Requirements, Agreed Project Plan, or other parts of the Contract, BMC shall use its best endeavors to assist the Supplier in obtaining such services in a timely and expeditious manner.

f. BMC shall be responsible for timely provision of all resources, access, and information necessary for the Installation and Operational Acceptance of the System (including, but not limited to, any required telecommunications or electric power services), as identified in the Agreed Project Plan, except where provision of such items is explicitly identified in the Contract as being the responsibility of the Supplier. Delay by BMC may result in an appropriate extension of the Time for Operational Acceptance.

g. Unless otherwise specified in the Contract or agreed upon by BMC and the Supplier, BMC shall provide sufficient, properly qualified operating and technical personnel, as required by the Supplier to properly carry out Delivery, Pre-commissioning, Installation, Commissioning, and Operational Acceptance, at or before the time specified in the Implementation Schedule and the Agreed Project Plan.

h. BMC will designate appropriate staff for the training courses to be given by the Supplier and shall make all appropriate logistical arrangements for such training as specified in the Technical Requirements, the Agreed Project Plan, or other parts of the Contract.

i. BMC assumes primary responsibility for the Operational Acceptance Test(s) for the System, in accordance with GCC Clause (Commissioning and Operational Acceptance), and shall be

responsible for the continued operation of the System after Operational Acceptance. However, this shall not limit in any way the Supplier's responsibilities after the date of Operational Acceptance otherwise specified in the Contract.

j. BMC is responsible for performing and safely storing timely and regular backups of its data and Software in accordance with accepted data management principles, except where such responsibility is clearly assigned to the Supplier elsewhere in the Contract.

k. All costs and expenses involved in the performance of the obligations under this GCC Clause (BMC's Responsibilities) shall be the responsibility of BMC, save those to be incurred by the Supplier with respect to the performance of the Operational Acceptance Test(s), in accordance with GCC Clause (Commissioning and Operational Acceptance).

l. BMC shall have no other Purchaser's responsibilities.

C. PAYMENT

11. Contract Price

a. The Contract Price shall be as specified in Article 2 (Contract Price and Terms of Payment) of the Contract Agreement.

b. The Contract Price shall be a firm lump sum not subject to any alteration, except in the event of a Change in the System pursuant to GCC Clause (Changes to the System) or to other clauses in the Contract;

c. The Supplier shall be deemed to have satisfied itself as to the correctness and sufficiency of the Contract Price, which shall, except as otherwise provided for in the Contract, cover all its obligations under the Contract.

12. **Terms of Payment**

a. The Supplier's request for payment shall be made to BMC in writing, accompanied by an invoice describing, as appropriate, the System or Subsystem(s), Delivered, Pre-commissioned, Installed, and Operationally Accepted, and by documents submitted pursuant to GCC Clause (Procurement, Delivery, and Transport) and upon fulfillment of other obligations stipulated in the Contract. **The Contract Price shall be paid as specified in the relevant section of Section – BMC's Requirements.**

b. No payment made by BMC herein shall be deemed to constitute acceptance by BMC of the System or any Subsystem(s).

~~c.~~ Payments shall be made by BMC, after submission of a valid invoice by the Supplier.

d. Payments shall be made in the currency(ies) specified in the Contract Agreement, pursuant to GCC Clause (BMC's Responsibilities). For Goods and Services supplied locally, payments shall be made in Indian Rupees (INR).

13. Securities

a. Issuance of Securities

The Supplier shall provide the securities specified below in favor of BMC at the times and in the amount, manner, and form specified below.

b. Performance Security

i. The Supplier shall, within thirty (30) days of the notification of Contract award, provide a security for the due performance of the Contract in the amount in Indian Rupees (INR)**,** failing which a penalty of Rs. 5000/- per day will be applicable to the bidder
ii. The security shall be a bank guarantee in the form provided in the Sample Contractual Forms Section of the bidding documents, or it shall be in another form acceptable to BMC.
iii. The security shall automatically become null and void once all the obligations of the Supplier under the Contract have been fulfilled, including, but not limited to, any obligations during the Warranty Period and any extensions to the period. The security shall be returned to the Supplier no later than ninety (90) days after its expiration.
iv. Upon Operational Acceptance of the entire System, the security shall be reduced to the amount **specified in the BDS,** on the date of such Operational Acceptance, so that the reduced security would only cover the remaining warranty obligations of the Supplier.

14. Taxes and Duties

a. For Goods or Services supplied from outside India, the Supplier shall be entirely responsible for all taxes, stamp duties, license fees, and other such levies imposed outside India.

b. For Goods or Services supplied locally, the Supplier shall be entirely responsible for all taxes, duties, license fees, etc., incurred until delivery of the contracted Goods or Services to BMC.

c. If any tax exemptions, reductions, allowances, or privileges may be available to the Supplier in India, BMC shall use its best efforts to enable the Supplier to benefit from any such tax savings to the maximum allowable extent.

d. For the purpose of the Contract, it is agreed that the Contract Price specified in Article 2 (Contract Price and Terms of Payment) of the Contract Agreement is based on the taxes, duties, levies, and charges prevailing at the date thirty (30) days prior to the date of bid submission in India (also called "Tax" in this GCC Clause (Taxes and Duties). If any Tax rates are increased or decreased, a new Tax is introduced, an existing Tax is abolished, or any change in interpretation or application of any Tax occurs in the course of the performance of the Contract, which was or will be assessed on the Supplier, its Subcontractors, or their employees in connection with performance of the Contract, an equitable adjustment to the Contract Price shall be made to fully take into account any such change by addition to or reduction from the Contract Price, as the case may be.

D. INTELLECTUAL PROPERTY

15. Copyright

a. The Intellectual Property Rights in all Standard Software and Standard Materials shall remain vested in the owner of such rights.

b. BMC agrees to restrict use, copying, or duplication of the Standard Software and Standard Materials in accordance with GCC Clause (Software License Agreements), except that additional copies of Standard Materials may be made by BMC for use within the scope of the project of which the System is a part, in the event that the Supplier does not deliver copies within thirty (30) days from receipt of a request for such Standard Materials.

c. BMC's contractual rights to use the Standard Software or elements of the Standard Software may not be assigned, licensed, or otherwise transferred voluntarily except in accordance with the relevant license agreement to a legally constituted successor organization (e.g., a reorganization of a public entity formally authorized by the government or through a merger or acquisition of a private entity).

d. The Intellectual Property Rights in all Custom Software and Custom Materials specified in Appendices 4 and 5 of the Contract Agreement (if any) shall, at the date of this Contract or on creation of the rights (if later than the date of this Contract), vest in BMC. The Supplier shall do and execute or arrange for the doing and executing of each necessary act, document, and thing that BMC may consider necessary or desirable to perfect the right, title, and interest of BMC in and to those rights. In respect of such Custom Software and Custom Materials, the Supplier shall ensure that the holder of a moral right in such an item does not assert it, and the Supplier shall, if requested to do so by BMC and where permitted by applicable law, ensure that the holder of such a moral right waives it.

16. Software License Agreements

a. Except to the extent that the Intellectual Property Rights in the Software vest in BMC, the Supplier hereby grants to BMC license to access and use the Software, including all inventions, designs, and marks embodied in the Software.

Such license to access and use the Software shall:

a. be:

i. nonexclusive;

ii. fully paid up and irrevocable (except that it shall terminate if the Contract terminates under relevant GCC Clauses (Termination);

iii. valid throughout the territory of India;

iv. subject to NO additional restrictions.

b. permit the Software to be:

i. used or copied for use on or with the computer(s) for which it was acquired (if specified in the Technical Requirements and/or the Supplier's bid), plus a backup computer(s) of the same or similar capacity, if the primary is(are) inoperative, and during a reasonable transitional period when use is being transferred between primary and backup;

ii. used or copied for use on or transferred to a replacement computer(s), (and use on the original and replacement computer(s) may be simultaneous during a reasonable transitional period) provided that, if the Technical Requirements and/or the Supplier's bid specifies a class of computer to which the license is restricted, the replacement computer(s) is(are) within that class;

c. if the nature of the System is such as to permit such access, accessed from other computers connected to the primary and/or backup computer(s) by means of a local or wide-area network or similar arrangement, and used on or copied for use on those other computers to the extent necessary to that access;

d. reproduced for safekeeping or backup purposes;

e. customized, adapted, or combined with other computer software for use by BMC, provided that derivative software incorporating any substantial part of the delivered, restricted Software shall be subject to same restrictions as are set forth in this Contract;

f. disclosed to, and reproduced for use by, support service suppliers and their subcontractors, (and BMC may sublicense such persons to use and copy for use the

Software) to the extent reasonably necessary to the performance of their support service contracts, subject to the same restrictions as are set forth in this Contract; and

g. disclosed to, and reproduced for use by, NO other parties.

b. The Supplier has the right to audit the Standard Software to verify compliance with the above license agreements. BMC will make available to the Supplier, within seven (7) days of a written request, accurate and up-to-date records of the number and location of copies, the number of authorized users, or any other relevant data required to demonstrate use of the Standard Software as per the license agreement. If and only if, expressly agreed in writing between BMC and the Supplier, BMC will allow, under a pre-specified agreed procedure, the execution of embedded software functions under Supplier's control, and unencumbered transmission of resulting information on software usage.

17. Confidential Information

a. The "Receiving Party" (either BMC or the Supplier) shall keep confidential and shall not, without the written consent of the other party to this Contract ("the Disclosing Party"), divulge to any third party any documents, data, or other information of a confidential nature ("Confidential Information") connected with this Contract, and furnished directly or indirectly by the Disclosing Party prior to or during performance, or following termination, of this Contract.
b. For the purposes of GCC Clause (Confidential Information), the Supplier is also deemed to be the Receiving Party of Confidential Information generated by the Supplier itself in the course of the performance of its obligations under the Contract and relating to the businesses, finances, suppliers, employees, or other contacts of BMC or BMC's use of the System.
c. Notwithstanding relevant GCC Clauses (Confidential Information):
    i. the Supplier may furnish to its Subcontractor Confidential Information of BMC to the extent reasonably required for the Subcontractor to perform its work under the Contract; and
    ii. BMC may furnish Confidential Information of the Supplier: (i) to its support service suppliers and their subcontractors to the extent reasonably required for them to perform their work under their support service contracts; and (ii) to its affiliates and subsidiaries,
    in which event the Receiving Party shall ensure that the person to whom it furnishes Confidential Information of the Disclosing Party is aware of and abides by the Receiving Party's obligations under this GCC Clause (Confidential Information) as if that person were party to the Contract in place of the Receiving Party.
d. BMC shall not, without the Supplier's prior written consent, use any Confidential Information received from the Supplier for any purpose other than the operation, maintenance and further development of the System. Similarly, the Supplier shall not, without BMC's prior written consent, use any Confidential Information received from BMC for any purpose other than those that are required for the performance of the Contract.
e. The obligation of a party under relevant GCC Clauses (Confidential Information) above, however, shall not apply to that information which:
    i. now or hereafter enters the public domain through no fault of the Receiving Party;
    ii. can be proven to have been possessed by the Receiving Party at the time of disclosure and that was not previously obtained, directly or indirectly, from the Disclosing Party;
    iii. otherwise lawfully becomes available to the Receiving Party from a third party that has no obligation of confidentiality.
f. The above provisions of this GCC Clause (Confidential Information) shall not in any way modify any undertaking of confidentiality given by either of the parties to this Contract prior to the date of the Contract in respect of the System or any part thereof.
g. The provisions of this GCC Clause (Confidential Information) shall survive the termination, for whatever reason, of the Contract for three (3) years.

E. Supply, Installation, Testing, Commissioning, and Acceptance of the System

18. Representatives

a. Project Manager

If the Project Manager is not named in the Contract, then within fourteen (14) days of the Effective Date, BMC shall appoint and notify the Supplier in writing of the name of the Project Manager. BMC may from time to time appoint some other person as the Project Manager in place of the person previously so appointed and shall give notice of the name of such other person to the Supplier without delay. No such appointment shall be made at such a time or in such a manner as to impede the progress of work on the System. Such appointment shall take effect only upon receipt of such notice by the Supplier. The Project Manager shall have the authority to represent BMC on all day-to-day matters relating to the System or arising from the Contract and shall normally be the person giving or receiving notices on behalf of BMC pursuant to GCC Clause (Notices).

b. Supplier's Representative

i. If the Supplier's Representative is not named in the Contract, then within fourteen (14) days of the Effective Date, the Supplier shall appoint the Supplier's Representative and shall request BMC in writing to approve the person so appointed. The request must be accompanied by a detailed curriculum vitae for the nominee, as well as a description of any other System or non-System responsibilities the nominee would retain while performing the duties of the Supplier's Representative. If BMC does not object to the appointment within fourteen (14) days, the Supplier's Representative shall be deemed to have been approved. If BMC objects to the appointment within fourteen (14) days giving the reason therefor, then the Supplier shall appoint a replacement within fourteen (14) days of such objection in accordance with this GCC Clause (Representatives).

ii. The Supplier's Representative shall have the authority to represent the Supplier on all day-to-day matters relating to the System or arising from the Contract, and shall normally be the person giving or receiving notices on behalf of the Supplier pursuant to GCC Clause (Notices).

iii. The Supplier shall not revoke the appointment of the Supplier's Representative without BMC's prior written consent, which shall not be unreasonably withheld. If BMC consents to such an action, the Supplier shall appoint another person of equal or superior qualifications as the Supplier's Representative, pursuant to the procedure set out in GCC Clause (Representatives).

iv. The Supplier's Representative and staff are obliged to work closely with BMC's Project Manager and staff, act within their own authority, and abide by directives issued by BMC that are consistent with the terms of the Contract. The Supplier's Representative is responsible for managing the activities of its personnel and any subcontracted personnel.

v. The Supplier's Representative may, subject to the approval of BMC (which shall not be unreasonably withheld), at any time delegate to any person any of the powers, functions, and authorities vested in him or her. Any such delegation may be revoked at any time. Any such delegation or revocation shall be subject to a prior notice signed by the Supplier's Representative and shall specify the powers, functions, and authorities thereby delegated or revoked. No such delegation or revocation shall take effect unless and until the notice of it has been delivered.

vi. Any act or exercise by any person of powers, functions and authorities so delegated to him or her in accordance with GCC Clause (Representatives) shall be deemed to be an act or exercise by the Supplier's Representative.

c. Objections and Removals

i. BMC may by notice to the Supplier object to any representative or person employed by the Supplier in the execution of the Contract who, in the reasonable opinion of BMC, may have behaved inappropriately, be incompetent, or be negligent. BMC shall provide evidence of the same, whereupon the Supplier shall remove such person from work on the System.

ii. If any representative or person employed by the Supplier is removed in accordance with GCC Clause (Representatives), the Supplier shall, where required, promptly appoint a replacement.

19. Project Plan

a. In close cooperation with BMC and based on the Preliminary Project Plan included in the Supplier's bid, the Supplier shall develop a Project Plan encompassing the activities specified in the Contract. The contents of the Project Plan shall be as specified in the Section – BMC's Requirements.

b. Within *thirty (30)* days from the Effective Date of the Contract, the Supplier shall present a Project Plan to BMC. BMC shall, within *fourteen (14)* days of receipt of the Project Plan, notify the Supplier of any respects in which it considers that the Project Plan does not adequately ensure that the proposed program of work, proposed methods, and/or proposed Information Technologies will satisfy the Technical Requirements (in this Clause, called "non-conformities" below). The Supplier shall, within *five (5)* days of receipt of such notification, correct the Project Plan and resubmit to BMC. BMC shall, within *five (5)* days of resubmission of the Project Plan, notify the Supplier of any remaining non-conformities. This procedure shall be repeated as necessary until the Project Plan is free from non-conformities. When the Project Plan is free from non-conformities, BMC shall provide confirmation in writing to the Supplier. This approved Project Plan ("the Agreed Project Plan") shall be contractually binding on BMC and the Supplier.

c. If required, the impact on the Implementation Schedule of modifications agreed during finalization of the Agreed Project Plan shall be incorporated in the Contract by amendment, in accordance with relevant GCC Clauses (Changes to the System) and (Extension of Time for Achieving Operational Acceptance).

d. The Supplier shall undertake to supply, install, test, and commission the System in accordance with the Agreed Project Plan and the Contract.

e. The Supplier shall submit to BMC Monthly Progress Reports summarizing:

i. results accomplished during the prior period;

ii. cumulative deviations to date from schedule of progress milestones as specified in the Agreed Project Plan;

iii. corrective actions to be taken to return to planned schedule of progress; proposed revisions to planned schedule;

iv. other issues and outstanding problems; proposed actions to be taken;

v. resources that the Supplier expects to be provided by BMC and/or actions to be taken by BMC in the next reporting period;

vi. other issues or potential problems the Supplier foresees that could impact on project progress and/or effectiveness.

f. The Supplier shall submit to BMC other (periodic) reports as specified in the Section – BMC's Requirements.

20. Subcontracting

a. Appendix 3 (List of Approved Subcontractors) to the Contract Agreement specifies critical items of supply or services and a list of Subcontractors for each item that are considered acceptable by BMC. If no Subcontractors are listed for an item, the Supplier shall prepare a list of Subcontractors it considers qualified and wishes to be added to the list for such items. The Supplier may from time to time propose additions to or deletions from any such list. The Supplier shall submit any such list or any modification to the list to BMC for its approval in sufficient time so as not to impede the progress of work on the System. BMC shall not withhold such approval unreasonably. Such approval by BMC of a Subcontractor(s) shall not relieve the Supplier from any of its obligations, duties, or responsibilities under the Contract.

b. The Supplier may, at its discretion, select and employ Subcontractors for such critical items from those Subcontractors listed pursuant to GCC Clause (Subcontracting). If the Supplier wishes to employ a Subcontractor not so listed, or subcontract an item not so listed, it must seek BMC's prior approval under GCC Clause (Subcontracting).

c. For items for which pre-approved Subcontractor lists have not been specified in Appendix 3 to the Contract Agreement, the Supplier may employ such Subcontractors as it may select, provided: (i) the Supplier notifies BMC in writing at least thirty (30) days prior to the proposed mobilization date for such Subcontractor; and (ii) by the end of this period either BMC has granted its approval in writing or fails to respond. The Supplier shall not engage any Subcontractor to which BMC has objected in writing prior to the end of the notice period. The absence of a written objection by BMC during the above specified period shall constitute formal acceptance of the proposed Subcontractor. Except to the extent that it permits the deemed approval of BMC of Subcontractors not listed in the Contract Agreement, nothing in this Clause, however, shall limit the rights and obligations of either BMC or Supplier as they are specified in relevant GCC Clauses (Subcontracting), or in Appendix 3 of the Contract Agreement.

21. Design and Engineering

a. Technical Specifications and Drawings

i. The Supplier shall execute the basic and detailed design and the implementation activities necessary for successful installation of the System in compliance with the provisions of the Contract or, where not so specified, in accordance with good industry practice.

The Supplier shall be responsible for any discrepancies, errors or omissions in the specifications, drawings, and other technical documents that it has prepared, whether such specifications, drawings, and other documents have been approved by the Project Manager or not, provided that such discrepancies, errors, or omissions are not because of inaccurate information furnished in writing to the Supplier by or on behalf of BMC.

ii. The Supplier shall be entitled to disclaim responsibility for any design, data, drawing, specification, or other document, or any modification of such design, drawings, specification, or other documents provided or designated by or on behalf of BMC, by giving a notice of such disclaimer to the Project Manager.

b. Codes and Standard

i. Wherever references are made in the Contract to codes and standards in accordance with which the Contract shall be executed, the edition or the revised version of such codes and standards current at the date thirty (30) days prior to date of bid submission shall apply. During Contract execution, any changes in such codes and standards shall be applied after approval by BMC and shall be treated in accordance with GCC Clause (Changes to the System).

c. Approval/Review of Controlling Technical Documents by the Project Manager

i. There will NO Controlling Technical Documents required. However, if the Section – BMC's Requirements specifies Controlling Technical Documents, the Supplier shall prepare and furnish such documents for the Project Manager's approval or review.

Any part of the System covered by or related to the documents to be approved by the Project Manager shall be executed only after the Project Manager's approval of these documents.

Relevant GCC Clauses (Design and Engineering) shall apply to those documents requiring the Project Manager's approval, but not to those furnished to the Project Manager for its review only.

ii. Within fourteen (14) days after receipt by the Project Manager of any document requiring the Project Manager's approval in accordance with GCC Clause ((Design and Engineering), the Project Manager shall either return one copy of the document to the Supplier with its approval endorsed on the document or shall notify the Supplier in writing of its disapproval of the document and the reasons for disapproval and the modifications that the Project Manager proposes. If the Project Manager fails to take such action within the fourteen (14) days, then the document shall be deemed to have been approved by the Project Manager.

iii. The Project Manager shall not disapprove any document except on the grounds that the document does not comply with some specified provision of the Contract or that it is contrary to good industry practice.

iv. If the Project Manager disapproves the document, the Supplier shall modify the document and resubmit it for the Project Manager's approval in accordance with GCC Clause (Design and Engineering). If the Project Manager approves the document subject to modification(s), the Supplier shall make the required modification(s), and the document shall then be deemed to have been approved, subject to GCC Clause (Design and Engineering). The procedure set out in relevant GCC Clauses (Design and Engineering) shall be repeated, as appropriate, until the Project Manager approves such documents.

v. If any dispute occurs between BMC and the Supplier in connection with or arising out of the disapproval by the Project Manager of any document and/or any modification(s) to a document that cannot be settled between the parties within a reasonable period, then, in case the Contract Agreement includes and names an Adjudicator, such dispute may be referred to the Adjudicator for determination in accordance with GCC Clause (Adjudicator). If such dispute is referred to an Adjudicator, the Project Manager shall give instructions as to whether and if so, how, performance of the Contract is to proceed. The Supplier shall proceed with the Contract in accordance with the Project Manager's instructions, provided that if the Adjudicator upholds the Supplier's view on the dispute and if BMC has not given notice under GCC Clause

(Adjudication), then the Supplier shall be reimbursed by BMC for any additional costs incurred by reason of such instructions and shall be relieved of such responsibility or liability in connection with the dispute and the execution of the instructions as the Adjudicator shall decide, and the Time for Achieving Operational Acceptance shall be extended accordingly.

vi. The Project Manager's approval, with or without modification of the document furnished by the Supplier, shall not relieve the Supplier of any responsibility or liability imposed upon it by any provisions of the Contract except to the extent that any subsequent failure results from modifications required by the Project Manager or inaccurate information furnished in writing to the Supplier by or on behalf of BMC.

vii. The Supplier shall not depart from any approved document unless the Supplier has first submitted to the Project Manager an amended document and obtained the Project Manager's approval of the document, pursuant to the provisions of this GCC Clause (Design and Engineering). If the Project Manager requests any change in any already approved document and/or in any document based on such an approved document, the provisions of GCC Clause (Changes to the System) shall apply to such request.

22. Procurement, Delivery, and Transport

a. Subject to related BMC's responsibilities pursuant to relevant GCC Clauses (BMC's Responsibilities) and (Taxes and Duties), the Supplier shall manufacture or procure and transport all the Information Technologies, Materials, and other Goods in an expeditious and orderly manner to the Project Site.

b. Delivery of the Information Technologies, Materials, and other Goods shall be made by the Supplier in accordance with the Technical Requirements.

c. Early or partial deliveries require the explicit written consent of BMC, which consent shall not be unreasonably withheld.

d. Transportation

   i. The Supplier shall provide such packing of the Goods as is required to prevent their damage or deterioration during shipment. The packing, marking, and documentation within and outside the packages shall comply strictly with BMC's instructions to the Supplier.

   ii. The Supplier will bear responsibility for and cost of transport to the Project Sites in accordance with the terms and conditions used in the specification of prices in the Price Schedules, including the terms and conditions of the associated Incoterms.

   iii. The Supplier shall be free to use transportation through carriers registered in any eligible country and to obtain insurance from any eligible source country.

e. The Supplier will provide BMC with shipping and other documents, as specified below:

   i. For Goods supplied from outside India:

   Upon shipment, the Supplier shall notify BMC and the insurance company contracted by the Supplier to provide cargo insurance by telex, cable, facsimile, electronic mail, or EDI with the full details of the shipment. The Supplier shall promptly send the following documents to BMC by mail or courier, as appropriate, with a copy to the cargo insurance company:

1. two copies of the Supplier's invoice showing the description of the Goods, quantity, unit price, and total amount;
2. usual transportation documents;
3. insurance certificate;
4. certificate(s) of origin; and
5. estimated time and point of arrival in India and at the site.

ii. For Goods supplied locally (i.e., from within India):

Upon shipment, the Supplier shall notify BMC by telex, cable, facsimile, electronic mail, or EDI with the full details of the shipment. The Supplier shall promptly send the following documents to BMC by mail or courier, as appropriate:

1. two copies of the Supplier's invoice showing the Goods' description, quantity, unit price, and total amount;
2. delivery note, railway receipt, or truck receipt;
3. certificate of insurance;
4. certificate(s) of origin; and
5. estimated time of arrival at the site.

f. Customs Clearance

i. The Supplier will bear responsibility for, and cost of, customs clearance into India in accordance the particular Incoterm(s) used for Goods supplied from outside India in the Price Schedules referred to by Article 2 of the Contract Agreement.

ii. In the event of delays in customs clearance that are not the fault of the Supplier, the Supplier shall be entitled to an extension in the Time for Achieving Operational Acceptance, pursuant to GCC Clause (Extension of Time for Achieving Operational Acceptance);

23. Product Upgrades

a. At any point during performance of the Contract, should technological advances be introduced by the Supplier for Information Technologies originally offered by the Supplier in its bid and still to be delivered, the Supplier shall be obligated to offer to BMC the latest versions of the available Information Technologies having equal or better performance or functionality at the same or lesser unit prices, pursuant to GCC Clause (Changes to the System).

b. At any point during performance of the Contract, for Information Technologies still to be delivered, the Supplier will also pass on to BMC any cost reductions and additional and/or improved support and facilities that it offers to other clients of the Supplier in India, pursuant to GCC Clause (Changes to the System).

c. During performance of the Contract, the Supplier shall offer to BMC all new versions, releases, and updates of Standard Software, as well as related documentation and technical support services, within thirty (30) days of their availability from the Supplier to other clients of the Supplier in India, and no later than three (3) months after they are released in the country of origin. In no case will the prices for these Software exceed those quoted by the Supplier in the Recurrent Costs tables in its bid.

d. During the Warranty Period, the Supplier will provide at no additional cost to BMC all new versions, releases, and updates for all Standard Software that are used in the System, within thirty (30) days of their availability from the Supplier to other clients of the Supplier in India, and no later than three(3) months after they are released in the country of origin of the Software.

e. BMC shall introduce all new versions, releases or updates of the Software within three (3) months of receipt of a production-ready copy of the new version, release, or update, provided that the new version, release, or update does not adversely affect System operation or performance or require extensive reworking of the System. In cases where the new version, release, or update adversely affects System operation or performance, or requires extensive reworking of the System, the Supplier shall continue to support and maintain the version or release previously in operation for as long as necessary to allow introduction of the new version, release, or update. In no case shall the Supplier stop supporting or maintaining a version or release of the Software less than twenty-four (24) months after BMC receives a production-ready copy of a subsequent version, release, or update. BMC shall use all reasonable endeavors to implement any new version, release, or update as soon as practicable, subject to the twenty-four-month-long stop date.

24. **Implementation, Installation, and Other Services**

a. The Supplier shall provide all Services specified in the Contract and Agreed Project Plan in accordance with the highest standards of professional competence and integrity.

b. Prices charged by the Supplier for Services, if not included in the Contract, shall be agreed upon in advance by the parties (including, but not restricted to, any prices submitted by the Supplier in the Recurrent Cost Schedules of its Bid) and shall not exceed the prevailing rates charged by the Supplier to other purchasers in India for similar services.

25. **Inspections and Tests**

a. BMC or its representative shall have the right to inspect and/or test any components of the System, as specified in the Technical Requirements, to confirm their good working order and/or conformity to the Contract at the point of delivery and/or at the Project Site.

b. BMC or its representative shall be entitled to attend any such inspections and/or tests of the components, provided that BMC shall bear all costs and expenses incurred in connection with such attendance, including but not limited to all inspection agent fees, travel, and related expenses.

c. Should the inspected or tested components fail to conform to the Contract, BMC may reject the component(s), and the Supplier shall either replace the rejected component(s), or make alterations as necessary so that it meets the Contract requirements free of cost to BMC.

d. The Project Manager may require the Supplier to carry out any inspection and/or test not specified in the Contract, provided that the Supplier's reasonable costs and expenses incurred in the carrying out of such inspection and/or test shall be added to the Contract Price. Further, if such inspection and/or test impedes the progress of work on the System and/or the Supplier's performance of its other obligations under the Contract, due allowance will be made in respect of the Time for Achieving Operational Acceptance and the other obligations so affected.

e. If any dispute shall arise between the parties in connection with or caused by an inspection and/or with regard to any component to be incorporated in the System that cannot be settled amicably between the parties within a reasonable period of time, either party may invoke the

process pursuant to GCC Clause (Settlement of Disputes), starting with referral of the matter to the Adjudicator in case an Adjudicator is included and named in the Contract Agreement.

26. **Installation of the System**

a. As soon as the System, or any Subsystem, has, in the opinion of the Supplier, been delivered, pre-commissioned, and made ready for Commissioning and Operational Acceptance Testing in accordance with the Technical Requirements, the Agreed Project Plan, the Supplier shall so notify BMC in writing.

b. The Project Manager shall, within fourteen (14) days after receipt of the Supplier's notice under GCC Clause (Installation of the System), either issue an Installation Certificate in the form specified in the Sample Contractual Forms Section in the bidding documents, stating that the System, or major component or Subsystem (if Acceptance by major component or Subsystem is specified pursuant to the GCC Clause (Commissioning and Operational Acceptance), has achieved Installation by the date of the Supplier's notice under GCC Clause (Installation of the System), or notify the Supplier in writing of any defects and/or deficiencies, including, but not limited to, defects or deficiencies in the interoperability or integration of the various components and/or Subsystems making up the System. The Supplier shall use all reasonable endeavors to promptly remedy any defect and/or deficiencies that the Project Manager has notified the Supplier of. The Supplier shall then promptly carry out retesting of the System or Subsystem and, when in the Supplier's opinion the System or Subsystem is ready for Commissioning and Operational Acceptance Testing, notify BMC in writing, in accordance with GCC Clause (Installation of the System). The procedure set out in this GCC Clause (Installation of the System) shall be repeated, as necessary, until an Installation Certificate is issued.

c. If the Project Manager fails to issue the Installation Certificate and fails to inform the Supplier of any defects and/or deficiencies within fourteen (14) days after receipt of the Supplier's notice under GCC Clause (Installation of the System), or if BMC puts the System or a Subsystem into production operation, then the System (or Subsystem) shall be deemed to have achieved successful Installation as of the date of the Supplier's notice or repeated notice, or when BMC put the System into production operation, as the case may be.

27. **Commissioning and Operational Acceptance**

a. Commissioning

i. Commissioning of the System (or Subsystem if specified pursuant to the GCC Clause (Commissioning and Operational Acceptance) shall be commenced by the Supplier:

1. immediately after the Installation Certificate is issued by the Project Manager, pursuant to GCC Clause (Installation of the System); or

2. as otherwise specified in the Technical Requirement or the Agreed Project Plan; or

3. immediately after Installation is deemed to have occurred, under GCC Clause (Installation of the System).

ii. BMC shall supply the operating and technical personnel and all materials and information reasonably required to enable the Supplier to carry out its obligations with respect to Commissioning.

Production use of the System or Subsystem(s) shall not commence prior to the start of formal Operational Acceptance Testing.

b. Operational Acceptance Tests
   i. The Operational Acceptance Tests (and repeats of such tests) shall be the primary responsibility of BMC (in accordance with GCC Clause (BMC's Responsibilities)), but shall be conducted with the full cooperation of the Supplier during Commissioning of the System (or major components or Subsystem[s]), to ascertain whether the System (or major component or Subsystem[s]) conforms to the Technical Requirements and meets the standard of performance quoted in the Supplier's bid, including, but not restricted to, the functional and technical performance requirements. The Operational Acceptance Tests during Commissioning will be conducted as specified in the Technical Requirements and/or the Agreed Project Plan.
   At BMC's discretion, Operational Acceptance Tests may also be performed on replacement Goods, upgrades and new version releases, and Goods that are added or field-modified after Operational Acceptance of the System.
   ii. If for reasons attributable to BMC, the Operational Acceptance Test of the System (or Subsystem[s] or major components, pursuant to the GCC Clause (Commissioning and Operational Acceptance)) cannot be successfully completed within ninety (90) days from the date of Installation or any other period agreed upon in writing by BMC and the Supplier, the Supplier shall be deemed to have fulfilled its obligations with respect to the technical and functional aspects of the Technical Specifications, and/or the Agreed Project Plan, and relevant GCC Clauses (Operational Acceptance Time Guarantee) shall not apply.

c. Operational Acceptance
   i. Subject to GCC Clause (Commissioning and Operational Acceptance – Sub-Clause Partial Acceptance) below, Operational Acceptance shall occur in respect of the System, when
      1. the Operational Acceptance Tests, as specified in the Technical Requirements, and/or the Agreed Project Plan have been successfully completed; or
      2. the Operational Acceptance Tests have not been successfully completed or have not been carried out for reasons that are attributable to BMC within the period from the date of Installation or any other agreed-upon period as specified in GCC Clause (Commissioning and Operational Acceptance) above; or
      3. BMC has put the System into production or use for sixty (60) consecutive days. If the System is put into production or use in this manner, the Supplier shall notify BMC and document such use.
   ii. At any time after any of the events set out in GCC Clause (Commissioning and Operational Acceptance) have occurred, the Supplier may give a notice to the Project Manager requesting the issue of an Operational Acceptance Certificate.
   iii. After consultation with BMC, and within fourteen (14) days after receipt of the Supplier's notice, the Project Manager shall:
      1. issue an Operational Acceptance Certificate; or
      2. notify the Supplier in writing of any defect or deficiencies or other reason for the failure of the Operational Acceptance Tests; or
      3. issue the Operational Acceptance Certificate, if the situation covered by GCC Clause (Commissioning and Operational Acceptance) arises.
   iv. The Supplier shall use all reasonable endeavors to promptly remedy any defect and/or deficiencies and/or other reasons for the failure of the Operational Acceptance Test that the Project Manager has notified the Supplier of. Once such remedies have been made by the Supplier, the Supplier shall notify BMC, and BMC, with the full cooperation of the Supplier, shall use all reasonable endeavors to promptly carry out retesting of the System or Subsystem. Upon the successful conclusion of the Operational Acceptance Tests, the Supplier shall notify BMC of its request for Operational Acceptance Certification, in accordance with GCC Clause (Commissioning and Operational Acceptance). BMC shall then issue to the Supplier the Operational Acceptance Certification in accordance with GCC Clause (Commissioning and Operational Acceptance), or shall notify the Supplier of further defects, deficiencies, or other reasons for the failure of the Operational Acceptance Test. The procedure set out in this GCC Clause (Commissioning and Operational Acceptance) shall be repeated, as necessary, until an Operational Acceptance Certificate is issued.

v. If the System or Subsystem fails to pass the Operational Acceptance Test(s) in accordance with GCC Clause (Commissioning and Operational Acceptance), then either:
   1. BMC may consider terminating the Contract, pursuant to GCC Clause (Termination); or
   2. if the failure to achieve Operational Acceptance within the specified time period is a result of the failure of BMC to fulfill its obligations under the Contract, then the Supplier shall be deemed to have fulfilled its obligations with respect to the relevant technical and functional aspects of the Contract, and relevant GCC Clauses (Functional Guarantees) shall not apply.

vi. If within fourteen (14) days after receipt of the Supplier's notice the Project Manager fails to issue the Operational Acceptance Certificate or fails to inform the Supplier in writing of the justifiable reasons why the Project Manager has not issued the Operational Acceptance Certificate, the System or Subsystem shall be deemed to have been accepted as of the date of the Supplier's said notice.

d. Partial Acceptance
   i. If so specified in this GCC Clause (Commissioning and Operational Acceptance), Installation and Commissioning shall be carried out individually for each identified major component or Subsystem(s) of the System. In this event, the provisions in the Contract relating to Installation and Commissioning, including the Operational Acceptance Test, shall apply to each such major component or Subsystem individually, and Operational Acceptance Certificate(s) shall be issued accordingly for each such major component or Subsystem of the System, subject to the limitations contained in GCC Clause (Commissioning and Operational Acceptance).
   ii. The issuance of Operational Acceptance Certificates for individual major components or Subsystems pursuant to GCC Clause (Commissioning and Operational Acceptance) shall not relieve the Supplier of its obligation to obtain an Operational Acceptance Certificate for the System as an integrated whole (if so specified in the GCC Clauses (Terms of Payment) and (Commissioning and Operational Acceptance)) once all major components and Subsystems have been supplied, installed, tested, and commissioned.
   iii. In the case of minor components for the System that by their nature do not require Commissioning or an Operational Acceptance Test (e.g., minor fittings, furnishings or site works, etc.), the Project Manager shall issue an Operational Acceptance Certificate within fourteen (14) days after the fittings and/or furnishings have been delivered and/or installed or the site works have been completed. The Supplier shall, however, use all reasonable endeavors to promptly remedy any defects or deficiencies in such minor components detected by BMC or Supplier.

F. GUARANTEES AND LIABILITIES

28. Operational Acceptance Time Guarantee

a. The Supplier guarantees that it shall complete the supply, Installation, Commissioning, and achieve Operational Acceptance of the System (or Subsystems, pursuant to the GCC Clause (Commissioning and Operational Acceptance) within the time periods specified in the Implementation Schedule and/or the Agreed Project Plan pursuant to GCC Clause (Time for Commencement and Acceptance), or within such extended time to which the Supplier shall be entitled under GCC Clause (Extension of Time for Achieving Operational Acceptance).

b. If the Supplier fails to supply, install, commission, and achieve Operational Acceptance of the System (or Subsystems pursuant to the GCC Clause (Commissioning and Operational Acceptance) within the time for achieving Operational Acceptance specified in the Implementation Schedule or the Agreed Project Plan, or any extension of the time for achieving Operational Acceptance previously granted under GCC Clause (Extension of Time for Achieving Operational Acceptance), the Supplier shall pay to BMC liquidated damages at the rate of one half of one percent per week as a percentage of the Contract Price (exclusive of Recurrent Costs

if any), or the relevant part of the Contract Price if a Subsystem has not achieved Operational Acceptance. The aggregate amount of such liquidated damages shall in no event exceed the amount of ten (10) percent of the Contract Price (exclusive of Recurrent Costs if any). Once the Maximum is reached, BMC may consider termination of the Contract, pursuant to GCC Clause (Termination).

c. Liquidated damages payable under GCC Clause (Operational Acceptance Time Guarantee) shall apply only to the failure to achieve Operational Acceptance of the System (and Subsystems) as specified in the Implementation Schedule and/or Agreed Project Plan. This Clause (Operational Acceptance Time Guarantee) shall not limit, however, any other rights or remedies BMC may have under the Contract for other delays.

d. If liquidated damages are claimed by BMC for the System (or Subsystem), the Supplier shall have no further liability whatsoever to BMC in respect to the Operational Acceptance time guarantee for the System (or Subsystem). However, the payment of liquidated damages shall not in any way relieve the Supplier from any of its obligations to complete the System or from any other of its obligations and liabilities under the Contract.

29. Defect Liability

a. The Supplier warrants that the System, including all Information Technologies, Materials, and other Goods supplied and Services provided, shall be free from defects in the design, engineering, Materials, and workmanship that prevent the System and/or any of its components from fulfilling the Technical Requirements or that limit in a material fashion the performance, reliability, or extensibility of the System and/or Subsystems. There will be NO exceptions and/or limitations to this warranty with respect to Software (or categories of Software). Commercial warranty provisions of products supplied under the Contract shall apply to the extent that they do not conflict with the provisions of this Contract.

b. The Supplier also warrants that the Information Technologies, Materials, and other Goods supplied under the Contract are new, unused, and incorporate all recent improvements in design that materially affect the System's or Subsystem's ability to fulfill the Technical Requirements.

c. The Supplier warrants that: (i) all Goods components to be incorporated into the System form part of the Supplier's and/or Subcontractor's current product lines, and (ii) they have been previously released to the market.

d. The Warranty Period shall commence from the date of Operational Acceptance of the System (or of any major component or Subsystem for which separate Operational Acceptance is provided for in the Contract).

e. If during the Warranty Period any defect as described in GCC Clause (Defect Liability) should be found in the design, engineering, Materials, and workmanship of the Information Technologies and other Goods supplied or of the Services provided by the Supplier, the Supplier shall promptly, in consultation and agreement with BMC regarding appropriate remedying of the defects, and at its sole cost, repair, replace, or otherwise make good (as the Supplier shall, at its discretion, determine) such defect as well as any damage to the System caused by such defect. Any defective Information Technologies or other Goods that have been replaced by the Supplier shall remain the property of the Supplier.

f. The Supplier shall not be responsible for the repair, replacement, or making good of any defect, or of any damage to the System arising out of or resulting from any of the following causes:

    i. improper operation or maintenance of the System by BMC;

ii. normal wear and tear;

iii. use of the System with items not supplied by the Supplier, unless otherwise identified in the Technical Requirements, or approved by the Supplier; or

iv. modifications made to the System by BMC, or a third party, not approved by the Supplier.

g. The Supplier's obligations under this GCC Clause (Defect Liability) shall not apply to:

i. any materials that are normally consumed in operation or have a normal life shorter than the Warranty Period; or

ii. any designs, specifications, or other data designed, supplied, or specified by or on behalf of BMC or any matters for which the Supplier has disclaimed responsibility, in accordance with GCC Clause (Design and Engineering).

h. BMC shall give the Supplier a notice promptly following the discovery of such defect, stating the nature of any such defect together with all available evidence. BMC shall afford all reasonable opportunity for the Supplier to inspect any such defect. BMC shall afford the Supplier all necessary access to the System and the site to enable the Supplier to perform its obligations under this GCC Clause (Defect Liability).

i. The Supplier may, with the consent of BMC, remove from the site any Information Technologies and other Goods that are defective, if the nature of the defect, and/or any damage to the System caused by the defect, is such that repairs cannot be expeditiously carried out at the site. If the repair, replacement, or making good is of such a character that it may affect the efficiency of the System, BMC may give the Supplier notice requiring that tests of the defective part be made by the Supplier immediately upon completion of such remedial work, whereupon the Supplier shall carry out such tests.

If such part fails the tests, the Supplier shall carry out further repair, replacement, or making good (as the case may be) until that part of the System passes such tests. The tests shall be agreed upon by BMC and the Supplier.

j. The response times and repair/replacement times for Warranty Defect Repair are specified in the Technical Requirements. Nevertheless, if the Supplier fails to commence the work necessary to remedy such defect or any damage to the System caused by such defect within two weeks BMC may, following notice to the Supplier, proceed to do such work or contract a third party (or parties) to do such work, and the reasonable costs incurred by BMC in connection with such work shall be paid to BMC by the Supplier or may be deducted by BMC from any monies due the Supplier or claimed under the Performance Security.

k. If the System or Subsystem cannot be used by reason of such defect and/or making good of such defect, the Warranty Period for the System shall be extended by a period equal to the period during which the System or Subsystem could not be used by BMC because of such defect and/or making good of such defect.

l. Items substituted for defective parts of the System during the Warranty Period shall be covered by the Defect Liability Warranty for the remainder of the Warranty Period applicable for the part replaced or three (3) months, whichever is greater. For reasons of information security, BMC may choose to retain physical possession of any replaced defective information storage devices.

m. At the request of BMC and without prejudice to any other rights and remedies that BMC may have against the Supplier under the Contract, the Supplier will offer all possible assistance to BMC to seek warranty services or remedial action from any subcontracted third-party

producers or licensor of Goods included in the System, including without limitation assignment or transfer in favor of BMC of the benefit of any warranties given by such producers or licensors to the Supplier.

30. Functional Guarantees

a. The Supplier guarantees that, once the Operational Acceptance Certificate(s) has been issued, the System represents a complete, integrated solution to BMC's requirements set forth in the Technical Requirements and it conforms to all other aspects of the Contract. The Supplier acknowledges that GCC Clause (Commissioning and Operational Acceptance) regarding Commissioning and Operational Acceptance governs how technical conformance of the System to the Contract requirements will be determined.

b. If, for reasons attributable to the Supplier, the System does not conform to the Technical Requirements or does not conform to all other aspects of the Contract, the Supplier shall at its cost and expense make such changes, modifications, and/or additions to the System as may be necessary to conform to the Technical Requirements and meet all functional and performance standards. The Supplier shall notify BMC upon completion of the necessary changes, modifications, and/or additions and shall request BMC to repeat the Operational Acceptance Tests until the System achieves Operational Acceptance.

c. If the System (or Subsystem[s]) fails to achieve Operational Acceptance, BMC may consider termination of the Contract, pursuant to GCC Clause (Termination), and forfeiture of the Supplier's Performance Security in accordance with GCC Clause (Securities) in compensation for the extra costs and delays likely to result from this failure.

31. Audit, Access and Reporting

a. Purpose

This GCC details the audit, access and reporting rights and obligations of the BMC or its nominated agency and the Supplier.

b. **Audit Notice and Timing**

i. As soon as reasonably practicable after the Effective Date, the Parties shall use their best endeavors to agree to a timetable for routine audits during the Project Implementation Phase and the Operation and Management Phase. Such timetable during the Implementation Phase, the BMC or its nominated agency and thereafter during the operation Phase, the BMC or its nominated agency shall conduct routine audits in accordance with such agreed timetable and shall not be required to give the Supplier any further notice of carrying out such audits.

ii. The BMC or its nominated agency may conduct non-timetabled audits at it's own discretion if it reasonably believes that such non-timetabled audits are necessary as a result of an act of fraud by the Supplier, a security violation, or breach of confidentiality obligations by the Supplier, provided that the requirement for such an audit is notified in writing to the Supplier a reasonable period time prior to the audit (taking into account the circumstances giving rise to the reasonable belief) stating in a reasonable level of detail the reasons for the requirement and the alleged facts on which the requirement is based.

iii. The frequency of audits shall be a (maximum) half yearly, provided always that the BMC or its nominated agency shall endeavor to conduct such audits with the lowest levels of inconvenience and disturbance practicable being caused to the Supplier. Any such audit shall be conducted by with adequate notice of 2 weeks to the Supplier.

c. Access

i. The Supplier shall provide to the BMC or its nominated agency reasonable access to employees, subcontractors, suppliers, agents and third-party facilities as detailed in the RFB, documents, records and systems reasonably required for audit and shall provide all such persons with routine assistance in connection with the audits and inspections. The Project Manager of BMC shall have the right to copy and retain copies of any relevant records. The Supplier shall make every reasonable effort to co-operate with them.

d. Audit Rights

i. The BMC or its nominated agency shall have the right to audit and inspect suppliers, agents and third party facilities (as detailed in the RFB), data centers, documents, records, procedures and systems relating to the provision of the services, but only to the extent that they relate to the provision of the services, as shall be reasonably necessary to verify:

1. The security, integrity and availability of all data processed, held or conveyed by the Partner on behalf of BMC and documentation related thereto;

2. That the actual level of performance of the services is the same as specified in the Service Level Agreement (SLA);

3. That the Supplier has complied with the relevant technical standards, and has adequate internal controls in place; and

4. The compliance of the Supplier with any other obligation under the Contract and SLA.

5. Security audit and implementation audit of the system shall be done once each year, the cost of which shall be borne by the Supplier.

6. For the avoidance of doubt the audit rights under this GCC shall not include access to the Supplier's profit margins or overheads, any confidential information relating to the Supplier' employees, or (iii) minutes of its internal Board or Board committee meetings including internal audit, or (iv) such other information of commercial-in-confidence nature which are not relevant to the Services associated with any obligation under the Contract.

e. Audit Rights of Sub-contractors, Suppliers and Agents

i. The Supplier shall use reasonable endeavors to achieve the same audit and access provisions as defined in this GCC with subcontractors who supply labor, services in respect of the services. The Supplier shall inform the BMC or its nominated agency prior to concluding any sub-contract or supply agreement of any failure to achieve the same rights of audit or access.

ii. REPORTING: The Supplier will provide quarterly reports to the Project Manager of BMC, regarding any specific aspects of the Project and in context of the audit and access information as required by the BMC or its nominated agency.

f. Action & Review

i. Any change or amendment to the systems and procedures of the Supplier, or sub-contractors, where applicable arising from the audit report shall be agreed within thirty (30) calendar days from the submission of the said report.

ii. Any discrepancies identified by any audit pursuant to this GCC shall be immediately notified to the BMC or its nominated agency and the Supplier Project Manager who shall determine what action should be taken in respect of such discrepancies in accordance with the terms of the Contract.

g. Terms of Payment

i. The BMC shall bear the cost of any audits and inspections. The terms of payment are exclusive of any costs of the Supplier and the sub-contractor, for all reasonable assistance and information provided under the Contract, the Project Implementation, Operation and Management SLA by the Supplier pursuant to this GCC.

h. Records and Information

i. For the purposes of audit in accordance with this GCC, the Supplier shall maintain true and accurate records in connection with the provision of the services and the Supplier shall handover all the relevant records and documents upon the termination or expiry of the Contract.

32. Intellectual Property Rights Warranty

a. The Supplier hereby represents and warrants that:

i. the System as supplied, installed, tested, and accepted;

ii. use of the System in accordance with the Contract; and

iii. copying of the Software and Materials provided to BMC in accordance with the Contract

iv. do not and will not infringe any Intellectual Property Rights held by any third party and that it has all necessary rights or at its sole expense shall have secured in writing all transfers of rights and other consents necessary to make the assignments, licenses, and other transfers of Intellectual Property Rights and the warranties set forth in the Contract, and for BMC to own or exercise all Intellectual Property Rights as provided in the Contract. Without limitation, the Supplier shall secure all necessary written agreements, consents, and transfers of rights from its employees and other persons or entities whose services are used for development of the System.

v. Bespoke development: Subject to the provisions of Clause v and vi below, upon payment, the IPR rights for any bespoke development done during the implementation of the project will lie exclusively with the BMC. [Note: Ministry of Electronic and Information Technology, Government of India, has notified “Policy on Collaborative Application Development by Opening the Source Code of Government Applications” in the Gazette of India on 6th May 2015. The same needs to be adopted.]

vi. Pre-existing work: All IPR including the source code and materials developed or otherwise obtained independently of the efforts of a Party under this Agreement (“pre-existing work”) including any enhancement or modification thereto shall remain the sole property of that Party. During the performance of the services for this agreement, each party grants to the other party (and their sub-contractors as necessary) a non-exclusive license to use, reproduce and modify any of its pre-existing work provided to the other party solely for the performance of such services for duration of the Term of this Agreement. Except as may be otherwise explicitly agreed to in a statement of services, upon payment in full, the Supplier should grant BMC a non-exclusive, perpetual, fully paid-up license to use the pre-existing work in the form delivered to BMC as part of the service or deliverables only for its internal business operations. Under such license, either of parties will have no right to sell the pre-existing work of the other party to a Third Party. BMC’s license to pre-existing work is conditioned upon its compliance

with the terms of this Agreement and the perpetual license applies solely to the pre-existing work that bidder leaves with BMC at the conclusion of performance of the services.

vii. Residuals: In no event shall Supplier be precluded from independently developing for itself, or for others, anything, whether in tangible or non-tangible form, which is competitive with, or similar to, the deliverables, set-out in this Agreement or Annexure. In addition, subject to the confidentiality obligations, Supplier shall be free to use its general knowledge, skills and experience, and any ideas, concepts, know-how, and techniques that are acquired or used in the course of providing the Services.

viii. The rights of the source code of the customized version of the COTS product shall lie with BMC. The source code needs to be transferred within three months of successful Operational Acceptance. All the costs associated with the transfer of source code shall be borne by the Supplier. This shall also include Octroi or customs to be paid for import/export of software.

1. All the documents shall be updated as per the last release of that module. The documents shall be reviewed by BMC or agency appointed by BMC. Implementation agency shall ensure that any disparity / lacunae found in the documents are rectified and revised documents are submitted for further review. The transfer of documentation to be considered as complete after BMC issues the completion certificate for the task.
2. Transfer of all the code files, supporting libraries, database scripts, libraries and metadata dictionary, procedures and supporting software components. Source Code to be exact replica of the Information System live on the production server.
3. Documentation of Step-by-Step procedure for recompilation of the Application shall be submitted by Supplier. The documentation shall enable BMC (or any third party appointed by BMC) to install, configure and recompile the application.
4. While submitting the Source Code files, Supplier shall submit the declaration that the Source code is of the same version which is on Production Environment and used for live operations. Supplier shall provide the environment to recompile the source code and provide access to the application to confirm that the Source Code is of the latest version and is same as that on the Production Environment.
5. Implementation agency shall conduct the necessary Knowledge transfer sessions to the technical staff provided by the BMC. The success criterion of training will be that IT team provided by BMC is able to recompile successfully the entire Information System on the test server independently.
6. The transfer of source code shall be an on-going exercise. As and when, a new version of Information System is deployed in production; the source code of the changed modules shall be transferred as per the above protocol to BMC. At the end of contract period or at the end of the complete development and deployment of all the change requests provided by BMC within the contract period or whichever is later, the entire source code shall be transferred in the same way.
7. BMC may conduct the (a) Software architecture and code review and (b) Security Audit of the Application; and necessary compliances are carried out before handing over the source code during exit management. Timelines for this compliance shall be jointly decided between BMC and Supplier.

33. Intellectual Property Rights Indemnity

a. The Supplier shall indemnify and hold harmless BMC and its employees and officers from and against any and all losses, liabilities, and costs (including losses, liabilities, and costs incurred in defending a claim alleging such a liability), that BMC or its employees or officers may suffer as a result of any infringement or alleged infringement of any Intellectual Property Rights by reason of:

i. installation of the System by the Supplier or the use of the System, including the Materials, in the country where the site is located;

ii. copying of the Software and Materials provided the Supplier in accordance with the Agreement; and

iii. sale of the products produced by the System in any country, except to the extent that such losses, liabilities, and costs arise as a result of BMC's breach of GCC Clause (Intellectual Property Rights Warranty).

b. Such indemnity shall not cover any use of the System, including the Materials, other than for the purpose indicated by or to be reasonably inferred from the Contract, any infringement resulting from the use of the System, or any products of the System produced thereby in association or combination with any other goods or services not supplied by the Supplier, where the infringement arises because of such association or combination and not because of use of the System in its own right.

c. Such indemnities shall also not apply if any claim of infringement:

i. is asserted by a parent, subsidiary, or affiliate of BMC's organization;

ii. is a direct result of a design mandated by BMC's Technical Requirements and the possibility of such infringement was duly noted in the Supplier's Bid; or

iii. results from the alteration of the System, including the Materials, by BMC or any persons other than the Supplier or a person authorized by the Supplier.

d. If any proceedings are brought or any claim is made against BMC arising out of the matters referred to in GCC Clause (Intellectual Property Rights Indemnity), BMC shall promptly give the Supplier notice of such proceedings or claims, and the Supplier may at its own expense and in BMC's name conduct such proceedings or claim and any negotiations for the settlement of any such proceedings or claim.

If the Supplier fails to notify BMC within thirty (30) days after receipt of such notice that it intends to conduct any such proceedings or claim, then BMC shall be free to conduct the same on its own behalf. Unless the Supplier has so failed to notify BMC within the thirty (30) days, BMC shall make no admission that may be prejudicial to the defense of any such proceedings or claim. BMC shall, at the Supplier's request, afford all available assistance to the Supplier in conducting such proceedings or claim and shall be reimbursed by the Supplier for all reasonable expenses incurred in so doing.

e. BMC shall indemnify and hold harmless the Supplier and its employees, officers, and Subcontractors from and against any and all losses, liabilities, and costs (including losses, liabilities, and costs incurred in defending a claim alleging such a liability) that the Supplier or its employees, officers, or Subcontractors may suffer as a result of any infringement or alleged infringement of any Intellectual Property Rights arising out of or in connection with any design, data, drawing, specification, or other documents or materials provided to the Supplier in connection with this Contract by BMC or any persons (other than the Supplier) contracted by BMC, except to the extent that such losses, liabilities, and costs arise as a result of the Supplier's breach of GCC Clause (Intellectual Property Rights Indemnity).

f. Such indemnity shall not cover

i. any use of the design, data, drawing, specification, or other documents or materials, other than for the purpose indicated by or to be reasonably inferred from the Contract;

ii. any infringement resulting from the use of the design, data, drawing, specification, or other documents or materials, or any products produced thereby, in association or combination with any other Goods or Services not provided by BMC or any other person contracted by BMC, where the infringement arises because of such association or combination and not because of the use of the design, data, drawing, specification, or other documents or materials in its own right.

g. Such indemnities shall also not apply:

i. if any claim of infringement is asserted by a parent, subsidiary, or affiliate of the Supplier's organization;

ii. to the extent that any claim of infringement is caused by the alteration, by the Supplier, or any persons contracted by the Supplier, of the design, data, drawing, specification, or other documents or materials provided to the Supplier by BMC or any persons contracted by BMC.

h. If any proceedings are brought or any claim is made against the Supplier arising out of the matters referred to in GCC Clause (Intellectual Property Rights Indemnity), the Supplier shall promptly give BMC notice of such proceedings or claims, and BMC may at its own expense and in the Supplier's name conduct such proceedings or claim and any negotiations for the settlement of any such proceedings or claim. If BMC fails to notify the Supplier within thirty (30) days after receipt of such notice that it intends to conduct any such proceedings or claim, then the Supplier shall be free to conduct the same on its own behalf. Unless BMC has so failed to notify the Supplier within the thirty (30) days, the Supplier shall make no admission that may be prejudicial to the defense of any such proceedings or claim. The Supplier shall, at BMC's request, afford all available assistance to BMC in conducting such proceedings or claim and shall be reimbursed by BMC for all reasonable expenses incurred in so doing.

34. **Limitation of Liability**

a. Provided the following does not exclude or limit any liabilities of either party in ways not permitted by applicable law:

i. the Supplier shall not be liable to BMC, whether in contract, tort, or otherwise, for any indirect or consequential loss or damage, loss of use, loss of production, or loss of profits or interest costs, provided that this exclusion shall not apply to any obligation of the Supplier to pay liquidated damages to BMC; and

ii. the aggregate liability of the Supplier to BMC, whether under the Contract, in tort or otherwise, shall not exceed the total Contract Price, provided that this limitation shall not apply to any obligation of the Supplier to indemnify BMC with respect to intellectual property rights infringement.

35. **Transfer of Ownership**

a. With the exception of Software and Materials, the ownership of the Information Technologies and other Goods shall be transferred to BMC at the time of Delivery or otherwise under terms that may be agreed upon and specified in the Contract Agreement.

b. Ownership and the terms of usage of the Software and Materials supplied under the Contract shall be governed by GCC Clause (Copyright) and any elaboration in the Technical Requirements.

c. Ownership of the Supplier's Equipment used by the Supplier and its Subcontractors in connection with the Contract shall remain with the Supplier or its Subcontractors.

36. **Care of the System**

a. BMC shall become responsible for the care and custody of the System or Subsystems upon their Delivery. BMC shall make good at its own cost any loss or damage that may occur to the System or Subsystems from any cause from the date of Delivery until the date of Operational Acceptance of the System or Subsystems, pursuant to GCC Clause (Commissioning and Operational Acceptance), excepting such loss or damage arising from acts or omissions of the Supplier, its employees, or subcontractors.

b. If any loss or damage occurs to the System or any part of the System by reason of:

i. (insofar as they relate to the country where the Project Site is located) nuclear reaction, nuclear radiation, radioactive contamination, a pressure wave caused by aircraft or other aerial objects, or any other occurrences that an experienced contractor could not reasonably foresee, or if reasonably foreseeable could not reasonably make provision for or insure against, insofar as such risks are not normally insurable on the insurance market and are mentioned in the general exclusions of the policy of insurance taken out under GCC Clause (Insurances);

ii. any use not in accordance with the Contract, by BMC or any third party;

iii. any use of or reliance upon any design, data, or specification provided or designated by or on behalf of BMC, or any such matter for which the Supplier has disclaimed responsibility in accordance with GCC Clause (Design and Engineering),

BMC shall pay to the Supplier all sums payable in respect of the System or Subsystems that have achieved Operational Acceptance, notwithstanding that the same be lost, destroyed, or damaged. If BMC requests the Supplier in writing to make good any loss or damage to the System thereby occasioned, the Supplier shall make good the same at the cost of BMC in accordance with GCC Clause (Changes to the System). If BMC does not request the Supplier in writing to make good any loss or damage to the System thereby occasioned, BMC shall either request a change in accordance with GCC Clause (Changes to the System), excluding the performance of that part of the System thereby lost, destroyed, or damaged, or, where the loss or damage affects a substantial part of the System, BMC shall terminate the Contract pursuant to GCC Clause (Termination).

c. BMC shall be liable for any loss of or damage to any Supplier's Equipment which BMC has authorized to locate within BMC's premises for use in fulfillment of Supplier's obligations under the Contract, except where such loss or damage arises from acts or omissions of the Supplier, its employees, or subcontractors.

37. **Loss of or Damage to Property; Accident or Injury to Workers; Indemnification**

a. The Supplier and each and every Subcontractor shall abide by the job safety, insurance, customs, and immigration measures prevalent and laws in force in India.

b. Subject to GCC Clause (Loss of or Damage to Property; Accident or Injury or Workers; Indemnification), the Supplier shall indemnify and hold harmless BMC and its employees and officers from and against any and all losses, liabilities and costs (including losses, liabilities, and costs incurred in defending a claim alleging such a liability) that BMC or its employees

or officers may suffer as a result of the death or injury of any person or loss of or damage to any property (other than the System, whether accepted or not) arising in connection with the supply, installation, testing, and Commissioning of the System and by reason of the negligence of the Supplier or its Subcontractors, or their employees, officers or agents, except any injury, death, or property damage caused by the negligence of BMC, its contractors, employees, officers, or agents.

c. If any proceedings are brought or any claim is made against BMC that might subject the Supplier to liability under GCC Clause (Loss of or Damage to Property; Accident or Injury or Workers; Indemnification), BMC shall promptly give the Supplier notice of such proceedings or claims, and the Supplier may at its own expense and in BMC's name conduct such proceedings or claim and any negotiations for the settlement of any such proceedings or claim. If the Supplier fails to notify BMC within thirty (30) days after receipt of such notice that it intends to conduct any such proceedings or claim, then BMC shall be free to conduct the same on its own behalf. Unless the Supplier has so failed to notify BMC within the thirty (30) working day period, BMC shall make no admission that may be prejudicial to the defense of any such proceedings or claim. BMC shall, at the Supplier's request, afford all available assistance to the Supplier in conducting such proceedings or claim and shall be reimbursed by the Supplier for all reasonable expenses incurred in so doing.

d. BMC shall indemnify and hold harmless the Supplier and its employees, officers, and Subcontractors from any and all losses, liabilities, and costs (including losses, liabilities, and costs incurred in defending a claim alleging such a liability) that the Supplier or its employees, officers, or Subcontractors may suffer as a result of the death or personal injury of any person or loss of or damage to property of BMC, other than the System not yet achieving Operational Acceptance, that is caused by fire, explosion, or any other perils, in excess of the amount recoverable from insurances procured under GCC Clause (Insurances), provided that such fire, explosion, or other perils were not caused by any act or failure of the Supplier.

e. If any proceedings are brought or any claim is made against the Supplier that might subject BMC to liability under GCC Clause (Loss of or Damage to Property; Accident or Injury or Workers; Indemnification), the Supplier shall promptly give BMC notice of such proceedings or claims, and BMC may at its own expense and in the Supplier's name conduct such proceedings or claim and any negotiations for the settlement of any such proceedings or claim. If BMC fails to notify the Supplier within thirty (30) days after receipt of such notice that it intends to conduct any such proceedings or claim, then the Supplier shall be free to conduct the same on its own behalf. Unless BMC has so failed to notify the Supplier within the thirty (30) days, the Supplier shall make no admission that may be prejudicial to the defense of any such proceedings or claim. The Supplier shall, at BMC's request, afford all available assistance to BMC in conducting such proceedings or claim and shall be reimbursed by BMC for all reasonable expenses incurred in so doing.

f. The party entitled to the benefit of an indemnity under this GCC Clause (Loss of or Damage to Property; Accident or Injury of Workers; Indemnification) shall take all reasonable measures to mitigate any loss or damage that has occurred. If the party fails to take such measures, the other party's liabilities shall be correspondingly reduced.

38. **Insurances**

a. The Supplier shall at its expense take out and maintain in effect, or cause to be taken out and maintained in effect, during the performance of the Contract, the insurance set forth below. The identity of the insurers and the form of the policies shall be subject to the approval of BMC, who should not unreasonably withhold such approval.

i. Cargo Insurance During Transport

as applicable, 110 percent of the price of the Information Technologies and other Goods in a freely convertible currency, covering the Goods from physical loss or damage during shipment through receipt at the Project Site.

ii. Installation "All Risks" Insurance

as applicable, 110 percent of the price of the Information Technologies and other Goods covering the Goods at the site from all risks of physical loss or damage (excluding only perils commonly excluded under "all risks" insurance policies of this type by reputable insurers) occurring prior to Operational Acceptance of the System.

iii. Third-Party Liability Insurance

The Supplier shall obtain Third-Party Liability Insurance in the amount equal to 110 percent of the price of the Information Technologies, and other Goods, covering bodily injury or death suffered by third parties (including BMC's personnel) and loss of or damage to property (including BMC's property and any Subsystems that have been accepted by BMC) occurring in connection with the supply and installation of the Information System. The Insurance shall cover the period from the Effective Date of the Contract till date of Operational Acceptance.

iv. Automobile Liability Insurance

In accordance with the statutory requirements prevailing in India, covering use of all vehicles used by the Supplier or its Subcontractors (whether or not owned by them) in connection with the execution of the Contract.

b. BMC shall be named as co-insured under all insurance policies taken out by the Supplier pursuant to GCC Clause (Insurances), except for the Third-Party Liability, and the Supplier's Subcontractors shall be named as co-insured under all insurance policies taken out by the Supplier pursuant to GCC Clause (Insurances) except for Cargo Insurance During Transport. All insurer's rights of subrogation against such co-insured for losses or claims arising out of the performance of the Contract shall be waived under such policies.

c. The Supplier shall deliver to BMC certificates of insurance (or copies of the insurance policies) as evidence that the required policies are in full force and effect.

d. The Supplier shall ensure that, where applicable, its Subcontractor(s) shall take out and maintain in effect adequate insurance policies for their personnel and vehicles and for work executed by them under the Contract, unless such Subcontractors are covered by the policies taken out by the Supplier.

e. If the Supplier fails to take out and/or maintain in effect the insurance referred to in GCC Clause (Insurances), BMC may take out and maintain in effect any such insurance and may from time to time deduct from any amount due the Supplier under the Contract any premium that BMC shall have paid to the insurer or may otherwise recover such amount as a debt due from the Supplier.

f. Unless otherwise provided in the Contract, the Supplier shall prepare and conduct all and any claims made under the policies affected by it pursuant to this GCC Clause (Insurances), and all monies payable by any insurers shall be paid to the Supplier. BMC shall give to the Supplier all such reasonable assistance as may be required by the Supplier in connection with any claim under the relevant insurance policies. With respect to insurance claims in

which BMC's interest is involved, the Supplier shall not give any release or make any compromise with the insurer without the prior written consent of BMC. With respect to insurance claims in which the Supplier's interest is involved, BMC shall not give any release or make any compromise with the insurer without the prior written consent of the Supplier.

39. **Force Majeure**

a. "Force Majeure" shall mean any event beyond the reasonable control of BMC or of the Supplier, as the case may be, and which is unavoidable notwithstanding the reasonable care of the party affected and shall include, without limitation, the following:

   i. war, hostilities, or warlike operations (whether a state of war be declared or not), invasion, act of foreign enemy, and civil war;

   ii. rebellion, revolution, insurrection, mutiny, usurpation of civil or military government, conspiracy, riot, civil commotion, and terrorist acts;

   iii. confiscation, nationalization, mobilization, commandeering or requisition by or under the order of any government or de jure or de facto authority or ruler, or any other act or failure to act of any local state or national government authority;

   iv. "strike, sabotage, lockout, embargo, import restriction, port congestion, lack of usual means of public transportation and communication, industrial dispute, shipwreck, shortage or restriction of power supply, epidemics, quarantine, and plague;

   v. earthquake, landslide, volcanic activity, fire, flood or inundation, tidal wave, typhoon or cyclone, hurricane, storm, lightning, or other inclement weather condition, nuclear and pressure waves, or other natural or physical disaster;

   vi. failure, by the Supplier, to obtain the necessary export permit(s) from the governments of the Country(s) of Origin of the Information Technologies or other Goods, or Supplier's Equipment provided that the Supplier has made all reasonable efforts to obtain the required export permit(s), including the exercise of due diligence in determining the eligibility of the System and all of its components for receipt of the necessary export permits.

b. If either party is prevented, hindered, or delayed from or in performing any of its obligations under the Contract by an event of Force Majeure, then it shall notify the other in writing of the occurrence of such event and the circumstances of the event of Force Majeure within fourteen (14) days after the occurrence of such event.

c. The party who has given such notice shall be excused from the performance or punctual performance of its obligations under the Contract for so long as the relevant event of Force Majeure continues and to the extent that such party's performance is prevented, hindered, or delayed. The Time for Achieving Operational Acceptance shall be extended in accordance with GCC Clause (Extension of Time for Achieving Operational Acceptance).

d. The party or parties affected by the event of Force Majeure shall use reasonable efforts to mitigate the effect of the event of Force Majeure upon its or their performance of the Contract and to fulfill its or their obligations under the Contract, but without prejudice to either party's right to terminate the Contract under GCC Clause (Force Majeure).

e. No delay or nonperformance by either party to this Contract caused by the occurrence of any event of Force Majeure shall:

   i. constitute a default or breach of the Contract;

ii. (subject to relevant GCC Clauses (Care of the System), (Force Majeure) give rise to any claim for damages or additional cost or expense occasioned by the delay or nonperformance

if, and to the extent that, such delay or nonperformance is caused by the occurrence of an event of Force Majeure.

f. If the performance of the Contract is substantially prevented, hindered, or delayed for a single period of more than sixty (60) days or an aggregate period of more than one hundred and twenty (120) days on account of one or more events of Force Majeure during the time period covered by the Contract, the parties will attempt to develop a mutually satisfactory solution, failing which, either party may terminate the Contract by giving a notice to the other.

g. In the event of termination pursuant to GCC Clause (Force Majeure), the rights and obligations of BMC and the Supplier shall be as specified in relevant GCC Clauses of (Termination).

h. Notwithstanding GCC Clause (Force Majeure), Force Majeure shall not apply to any obligation of BMC to make payments to the Supplier under this Contract.

40. Risk Purchase Clause

In the event the Supplier fails to execute the project as stipulated in the Contract, or as per the directions given by BMC from time to time, BMC reserves the right to procure similar services from the next eligible Bidder or from alternate sources at the cost of the Supplier. Before taking such a decision, BMC shall serve a notice period of one month to the Supplier. The 30 day notice period shall be considered as the 'Cure Period' to facilitate the Supplier to cure the breach. The provision for Risk Purchase shall be evoked in the event the Supplier fails to correct the breach within the 'Cure Period'. Further, the Supplier liability to pay shall be set as 25% of the value of the undelivered services.

H. CHANGE IN CONTRACT ELEMENTS

41. Changes to the System

a. Introducing a Change

i. Subject to this GCC Clauses (Changes to the System), BMC shall have the right to propose, and subsequently require, the Project Manager to order the Supplier from time to time during the performance of the Contract to make any change, modification, addition, or deletion to, in, or from the System (interchangeably called "Change"), provided that such Change falls within the general scope of the System, does not constitute unrelated work, and is technically practicable, taking into account both the state of advancement of the System and the technical compatibility of the Change envisaged with the nature of the System as originally specified in the Contract.

A Change may involve, but is not restricted to, the substitution of updated Information Technologies and related Services in accordance with GCC Clause (Product Upgrades).

ii. The Supplier may from time to time during its performance of the Contract propose to BMC (with a copy to the Project Manager) any Change that the Supplier considers necessary or desirable to improve the quality or efficiency of the System. BMC may at its discretion approve or reject any Change proposed by the Supplier.

iii. Notwithstanding relevant GCC Clauses (Changes to the System), no change made necessary because of any default of the Supplier in the performance of its obligations under the Contract shall be deemed to be a Change, and such change shall not result

in any adjustment of the Contract Price or the Time for Achieving Operational Acceptance.

iv. The procedure on how to proceed with and execute Changes is specified in these GCC Clauses of (Changes to the System), and further details and sample forms are provided in the Section - Contract Forms in the bidding documents.

v. Moreover, BMC and Supplier will agree, during development of the Project Plan, to a date prior to the scheduled date for Operational Acceptance, after which the Technical Requirements for the System shall be "frozen." Any Change initiated after this time will be dealt with after Operational Acceptance.

b. Changes Originating from BMC

i. If BMC proposes a Change pursuant to GCC Clauses (Changes to the System), it shall send to the Supplier a "Request for Change Proposal," requiring the Supplier to prepare and furnish to the Project Manager as soon as reasonably practicable a "Change Proposal," which shall include the following:

1. brief description of the Change;
2. impact on the Time for Achieving Operational Acceptance;
3. detailed estimated cost of the Change;
4. effect on Functional Guarantees (if any);
5. effect on any other provisions of the Contract.

ii. Upon receipt of the Supplier's Change Estimate Proposal, BMC shall do one of the following:

1. accept the Supplier's estimate with instructions to the Supplier to proceed with the preparation of the Change Proposal;
2. advise the Supplier of any part of its Change Estimate Proposal that is unacceptable and request the Supplier to review its estimate;
3. advise the Supplier that BMC does not intend to proceed with the Change.

iii. Upon receipt of BMC's instruction to proceed under relevant GCC Clause (Changes to the System), the Supplier shall, with proper expedition, proceed with the preparation of the Change Proposal, in accordance with GCC Clause (Changes to the System). The Supplier, at its discretion, may specify a validity period for the Change Proposal, after which if BMC and Supplier has not reached agreement in accordance with GCC Clause (Changes to the System), then BMC shall not intend to proceed with the Change.

iv. The pricing of any Change shall, as far as practicable, be calculated in accordance with the rates and prices included in the Contract. If the nature of the Change is such that the Contract rates and prices are inequitable, the parties to the Contract shall agree on other specific rates to be used for valuing the Change.

v. If before or during the preparation of the Change Proposal it becomes apparent that the aggregate impact of compliance with the Request for Change Proposal and with all other Change Orders that have already become binding upon the Supplier under this GCC Clause (Changes to the System) would be to increase or decrease the Contract Price as originally set forth in Article 2 (Contract Price) of the Contract Agreement by more than fifteen (15) percent, the Supplier may give a written notice

of objection to this Request for Change Proposal prior to furnishing the Change Proposal. If BMC accepts the Supplier's objection, BMC shall withdraw the proposed Change and shall notify the Supplier in writing of its acceptance.

The Supplier's failure to so object to a Request for Change Proposal shall neither affect its right to object to any subsequent requested Changes or Change Orders, nor affect its right to take into account, when making such subsequent objection, the percentage increase or decrease in the Contract Price that any Change not objected to by the Supplier represents.

~~vi.~~ Upon receipt of the Change Proposal, BMC and the Supplier shall mutually agree upon all matters contained in the Change Proposal. Within fourteen (14) days after such agreement, BMC shall, if it intends to proceed with the Change, issue the Supplier a Change Order. If BMC is unable to reach a decision within fourteen (14) days, it shall notify the Supplier with details of when the Supplier can expect a decision. If BMC decides not to proceed with the Change for whatever reason, it shall, within the said period of fourteen (14) days, notify the Supplier accordingly.

vii. If BMC and the Supplier cannot reach agreement on the price for the Change, an equitable adjustment to the Time for Achieving Operational Acceptance, or any other matters identified in the Change Proposal, the Change will not be implemented. However, this provision does not limit the rights of either party under GCC Clause (Settlement of Disputes).

c. Changes Originating from Supplier

If the Supplier proposes a Change pursuant to relevant GCC Clause (Changes to the System), the Supplier shall submit to the Project Manager a written "Application for Change Proposal," giving reasons for the proposed Change and including the information specified in the relevant GCC Clause (Changes to the System)1. Upon receipt of the Application for Change Proposal, the parties shall follow the procedures outlined in relevant GCC Clauses (Changes to the System).

42. **Extension of Time for Achieving Operational Acceptance**

a. The time(s) for achieving Operational Acceptance specified in the Schedule of Implementation shall be extended if the Supplier is delayed or impeded in the performance of any of its obligations under the Contract by reason of any of the following:

i. any Change in the System as provided in GCC Clause (Change in the Information System);

ii. any occurrence of Force Majeure as provided in GCC Clause (Force Majeure);

iii. default of BMC; or

iv. any other matter specifically mentioned in the Contract;

by such period as shall be fair and reasonable in all the circumstances and as shall fairly reflect the delay or impediment sustained by the Supplier.

b. Except where otherwise specifically provided in the Contract, the Supplier shall submit to the Project Manager a notice of a claim for an extension of the time for achieving Operational Acceptance, together with particulars of the event or circumstance justifying such extension as soon as reasonably practicable after the commencement of such event or circumstance. As soon as reasonably practicable after receipt of such notice and supporting particulars of

the claim, BMC and the Supplier shall agree upon the period of such extension. In the event that the Supplier does not accept BMC's estimate of a fair and reasonable time extension, the Supplier shall be entitled to refer the matter to the provisions for the Settlement of Disputes pursuant to GCC Clause (Fraud and Corruption).

c. The Supplier shall at all times use its reasonable efforts to minimize any delay in the performance of its obligations under the Contract.

43. **Termination**

a. Termination for BMC's Convenience

i. BMC may at any time terminate the Contract for any reason by giving the Supplier a notice of termination that refers to this GCC Clause (Termination).

ii. Upon receipt of the notice of termination under this GCC Clause (Termination), the Supplier shall either as soon as reasonably practical or upon the date specified in the notice of termination

1. cease all further work, except for such work as BMC may specify in the notice of termination for the sole purpose of protecting that part of the System already executed, or any work required to leave the site in a clean and safe condition;

2. terminate all subcontracts, except those to be assigned to BMC pursuant to this GCC Clause (Termination) (ii) below;

3. remove all Supplier's Equipment from the site, repatriate the Supplier's and its Subcontractors' personnel from the site, remove from the site any wreckage, rubbish, and debris of any kind;

4. in addition, the Supplier, subject to the payment specified in this GCC Clause (Termination), shall

a. deliver to BMC the parts of the System executed by the Supplier up to the date of termination;

b. to the extent legally possible, assign to BMC all right, title, and benefit of the Supplier to the System, or Subsystem, as at the date of termination, and, as may be required by BMC, in any subcontracts concluded between the Supplier and its Subcontractors;

c. deliver to BMC all nonproprietary drawings, specifications, and other documents prepared by the Supplier or its Subcontractors as of the date of termination in connection with the System.

iii. In the event of termination of the Contract under this GCC Clause (Termination), BMC shall pay to the Supplier the following amounts:

1. the Contract Price, properly attributable to the parts of the System executed by the Supplier as of the date of termination;

b. Termination for Supplier's Default

i. BMC, without prejudice to any other rights or remedies it may possess, may terminate the Contract forthwith in the following circumstances by giving a notice of termination and its reasons therefore to the Supplier, referring to this GCC Clause (Termination):

1. if the Supplier becomes bankrupt or insolvent, has a receiving order issued against it, compounds with its creditors, or, if the Supplier is a corporation, a

resolution is passed or order is made for its winding up (other than a voluntary liquidation for the purposes of amalgamation or reconstruction), a receiver is appointed over any part of its undertaking or assets, or if the Supplier takes or suffers any other analogous action in consequence of debt;

2. if the Supplier assigns or transfers the Contract or any right or interest therein in violation of the provision of GCC Clause (Assignment); or

ii. If the Supplier:

1. has abandoned or repudiated the Contract;
2. has without valid reason failed to commence work on the System promptly;
3. persistently fails to execute the Contract in accordance with the provisions of the Contract or persistently neglects to carry out its obligations under the Contract without just cause;
4. refuses or is unable to provide sufficient Materials, Services, or labor to execute and complete the System in the manner specified in the Agreed Project Plan furnished under GCC Clause (Project Plan) at rates of progress that give reasonable assurance to BMC that the Supplier can attain Operational Acceptance of the System by the Time for Achieving Operational Acceptance as extended;

then BMC may, without prejudice to any other rights it may possess under the Contract, give a notice to the Supplier stating the nature of the default and requiring the Supplier to remedy the same. If the Supplier fails to remedy or to take steps to remedy the same within fourteen (14) days of its receipt of such notice, then BMC may terminate the Contract forthwith by giving a notice of termination to the Supplier that refers to this GCC Clause (Termination).

iii. Upon receipt of the notice of termination under GCC Clauses (Termination), the Supplier shall, either immediately or upon such date as is specified in the notice of termination:

1. cease all further work, except for such work as BMC may specify in the notice of termination for the sole purpose of protecting that part of the System already executed or any work required to leave the site in a clean and safe condition;
2. terminate all subcontracts, except those to be assigned to BMC pursuant to GCC Clause (Termination) below;
3. deliver to BMC the parts of the System executed by the Supplier up to the date of termination;
4. to the extent legally possible, assign to BMC all right, title and benefit of the Supplier to the System or Subsystems as at the date of termination, and, as may be required by BMC, in any subcontracts concluded between the Supplier and its Subcontractors;
5. deliver to BMC all drawings, specifications, and other documents prepared by the Supplier or its Subcontractors as at the date of termination in connection with the System.

iv. BMC may enter upon the site, expel the Supplier, and complete the System itself or by employing any third party. Upon completion of the System or at such earlier date as BMC thinks appropriate, BMC shall give notice to the Supplier that such Supplier's

Equipment will be returned to the Supplier at or near the site and shall return such Supplier's Equipment to the Supplier in accordance with such notice. The Supplier shall thereafter without delay and at its cost remove or arrange removal of the same from the site.

v. Subject to GCC Clause (Termination), the Supplier shall be entitled to be paid the Contract Price attributable to the portion of the System executed as at the date of termination and the costs, if any, incurred in protecting the System and in leaving the site in a clean and safe condition pursuant to GCC Clause (Termination). Any sums due BMC from the Supplier accruing prior to the date of termination shall be deducted from the amount to be paid to the Supplier under this Contract.

vi. If BMC completes the System, the cost of completing the System by BMC shall be determined. If the sum that the Supplier is entitled to be paid, pursuant to GCC Clause (Termination), plus the reasonable costs incurred by BMC in completing the System, exceeds the Contract Price, the Supplier shall be liable for such excess. If such excess is greater than the sums due the Supplier under GCC Clause (Termination), the Supplier shall pay the balance to BMC, and if such excess is less than the sums due the Supplier under GCC Clause (Termination), BMC shall pay the balance to the Supplier. BMC and the Supplier shall agree, in writing, on the computation described above and the manner in which any sums shall be paid.

c. In this GCC Clause (Termination), the expression "portion of the System executed" shall include all work executed, Services provided, and all Information Technologies, or other Goods acquired (or subject to a legally binding obligation to purchase) by the Supplier and used or intended to be used for the purpose of the System, up to and including the date of termination.

d. In this GCC Clause (Termination), in calculating any monies due from BMC to the Supplier, account shall be taken of any sum previously paid by BMC to the Supplier under the Contract, including any advance payment paid.

44. Exit Management

a. **Purpose**

i. This GCC sets out the provisions, which will apply on expiry or termination of the Contract, the Project Implementation, Operation and Management Service Level Agreement (SLA).

ii. In the case of termination of the Project Implementation and/or Operation and Management, the Parties shall agree at that time whether, and if so during what period, the provisions of this GCC shall apply.

iii. The Parties shall ensure that their respective associated entities carry out their respective obligations set out in this GCC (Exit Management).

b. Transfer of Assets

i. BMC shall be entitled to serve notice in writing on the Supplier at any time during the exit management period as detailed hereinabove requiring the Supplier and/or its sub-contractors to provide the BMC with a complete and up to date list of the Assets within 30 days of such notice. BMC shall then be entitled to serve notice in writing on the Supplier at any time prior to a date that is 30 days prior to the end of the exit management period requiring the Supplier to sell the Assets (if any), to be transferred

to BMC or its nominated agencies at book value as determined as of the date of such notice in accordance with the provisions of relevant laws.

ii. In case of contract being terminated by BMC, BMC reserves the right to ask Supplier to continue running the project operations for a period of 6 months after termination orders are issued.

iii. Upon service of a notice under this GCC, the following provisions shall apply:

1. in the event, if the Assets to be transferred are mortgaged to any financial institutions by the Supplier, the Supplier shall ensure that all such liens and liabilities have been cleared beyond doubt, prior to such transfer. All documents regarding the discharge of such lien and liabilities shall be furnished to the BMC.
2. All risk in and title to the Assets to be transferred / to be purchased by the BMC pursuant to this GCC shall be transferred to BMC, on the last day of the exit management period.
3. BMC shall pay to the Supplier on the last day of the exit management period such sum representing the Net Block (procurement price less depreciation as per provisions of Companies Act) of the Assets to be transferred as stated in the Terms of Payment Schedule, if any.
4. Payment to the outgoing Supplier shall be made to the tune of the last set of completed services / deliverables, subject to SLA requirements.
5. The outgoing Supplier will pass on to BMC and/or to the Replacement Supplier, the subsisting rights in any leased properties/ licensed products on terms not less favorable to BMC/ Replacement Supplier, than that enjoyed by the outgoing Supplier.

c. Cooperation and Provision of Information

i. During the exit management period:

1. The Supplier will allow the BMC or its nominated agency access to information reasonably required to define the then current mode of operation associated with the provision of the services to enable the BMC to assess the existing services being delivered;
2. promptly on reasonable request by the BMC, the Supplier shall provide access to and copies of all information held or controlled by them which the Supplier have prepared or maintained in accordance with the contract, relating to any material aspect of the services (whether provided by the Supplier or sub-contractors appointed by the Supplier). The BMC shall be entitled to a copy of all such information. Such information shall include details pertaining to the services rendered and other performance data. The Supplier shall permit the BMC or its nominated agencies to have reasonable access to its employees and facilities as reasonably required to understand the methods of delivery of the services employed by the Supplier and to assist appropriate knowledge transfer.

d. Confidential Information, Security and Data

i. The Supplier will promptly on the commencement of the exit management period supply to the BMC or its nominated agency the following:

1. information relating to the current services rendered to the citizens / customer and performance data relating to the performance of sub-contractors in relation to the services;
2. documentation relating to Information System Project's Intellectual Property Rights;
3. documentation relating to sub-contractors;

4. all current and updated data as is reasonably required for purposes of BMC or its nominated agencies transitioning the services to its Replacement Supplier in a readily available format nominated by the BMC or its nominated agency;
5. all other information (including but not limited to documents, records and agreements) relating to the services reasonably necessary to enable BMC or its nominated agencies, or its Replacement Supplier to carry out due diligence in order to transition the provision of the Services to BMC or its nominated agencies, or its Replacement Supplier (as the case may be)

ii. Before the expiry of the exit management period, the Supplier shall deliver to the BMC or its nominated agency all new or up-dated materials from the categories set out in the Contract and shall not retain any copies thereof, except that the Supplier shall be permitted to retain one copy of such materials for archival purposes only.

iii. Before the expiry of the exit management period, unless otherwise provided under the Contract, the BMC or its nominated agency shall deliver to the Supplier all forms of Suppliers confidential information, which is in the possession or control of BMC.

e. Employees

i. Promptly on reasonable request at any time during the exit management period, the Suppliers shall, subject to applicable laws, restraints and regulations (including in particular those relating to privacy) provide to the BMC or its nominated agency a list of all employees (with job titles) of the Supplier dedicated to providing the services at the commencement of the exit management period.

ii. Where any national, regional law or regulation relating to the mandatory or automatic transfer of the contracts of employment from the Supplier to the BMC or its nominated agency, or a Replacement Supplier ("Transfer Regulation") applies to any or all of the employees of the Supplier then the Parties shall comply with their respective obligations under such Transfer Regulations.

f. Transfer of Certain Agreements

On request by the BMC or its nominated agency, the Supplier shall effect such assignments, transfers, licences and sub-licences as the Project Manager of BMC may require in favour of the BMC or its Replacement Supplier in relation to any equipment lease, maintenance or service provision agreement between Supplier and third party lessors, vendors, and which are related to the services and reasonably necessary for the carrying out of replacement services by the BMC or its nominated agency or its Replacement Supplier.

g. Rights of Access to Premises

i. At any time during the exit management period, where Assets are located at the Supplier's premises, the Supplier will be obliged to give reasonable rights of access to (or, in the case of Assets located on a third party's premises, procure reasonable rights of access to) the BMC or its nominated agency and/or any Replacement Supplier in order to make an inventory of the Assets.

ii. The Supplier shall also give the BMC or its nominated agency or its nominated agencies, or any Replacement Supplier right of reasonable access to the Implementation Partner's premises and shall procure the BMC or its nominated agency or its nominated agencies and any Replacement Supplier rights of access to relevant third party premises during the exit management period and for such period of time following termination or expiry of the CONTRACT as is reasonably necessary to migrate the services to the BMC or its nominated agency, or a Replacement Supplier.

h. **General Obligations of the Supplier**

i. The Supplier shall provide all such information as may reasonably be necessary to effect as seamless a handover as practicable in the circumstances to the BMC or its nominated agency or its Replacement Supplier and which the Supplier has in its possession or control at any time during the exit management period.

ii. For the purposes of this GCC, anything in the possession or control of any Supplier, associated entity, or sub-contractor is deemed to be in the possession or control of the Supplier.

iii. The Supplier shall commit adequate resources to comply with its obligations under this Exit Management GCC.

i. Exit Management Plan

i. The Supplier shall provide the BMC or its nominated agency with a recommended exit management plan ("Exit Management Plan") which shall deal with at least the following aspects of exit management in relation to the CONTRACT as a whole and in relation to the Project Implementation, and the Operation and Management SLA.

1. A detailed program of the transfer process that could be used in conjunction with a Replacement Supplier including details of the means to be used to ensure continuing provision of the services throughout the transfer process or until the cessation of the services and of the management structure to be used during the transfer;

2. plans for the communication with such of the Supplier's sub contractors, staff, suppliers, customers and any related third party as are necessary to avoid any material detrimental impact on the BMC's operations as a result of undertaking the transfer;

3. (if applicable) proposed arrangements for the segregation of the Supplier's networks from the networks employed by BMC and identification of specific security tasks necessary at termination;

4. Plans for provision of contingent support to BMC, and Replacement Supplier for a reasonable period after transfer.

ii. The Supplier shall re-draft the Exit Management Plan annually thereafter to ensure that it is kept relevant and up to date.

iii. Each Exit Management Plan shall be presented by the Supplier to and approved by the BMC or its nominated agencies.

iv. The terms of payment as stated in the Terms of Payment Schedule include the costs of the Supplier complying with its obligations under this GCC.

v. In the event of termination or expiry of CONTRACT, and Project Implementation, each Party shall comply with the Exit Management Plan.

vi. During the exit management period, the Supplier shall use its best efforts to deliver the services

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

viii. This Exit Management plan shall be furnished in writing to the BMC or its nominated agencies within 90 days from the Effective Date of this Contract**.**

45. Assignment

a. Neither BMC nor the Supplier shall, without the express prior written consent of the other, assign to any third party the Contract or any part thereof, or any right, benefit, obligation, or interest therein or thereunder, except that the Supplier shall be entitled to assign either absolutely or by way of charge any monies due and payable to it or that may become due and payable to it under the Contract.

46. Settlement of Disputes

a. Adjudication

i. If any dispute of any kind whatsoever shall arise between BMC and the Supplier in connection with or arising out of the Contract, including without prejudice to the generality of the foregoing, any question regarding its existence, validity, or termination, or the operation of the System (whether during the progress of

implementation or after its achieving Operational Acceptance and whether before or after the termination, abandonment, or breach of the Contract), the parties shall seek to resolve any such dispute by mutual consultation. If the parties fail to resolve such a dispute by mutual consultation within fourteen (14) days after one party has notified the other in writing of the dispute, then, if the Contract Agreement in Appendix 2 includes and names an Adjudicator, the dispute shall, within another fourteen (14) days, be referred in writing by either party to the Adjudicator, with a copy to the other party. If there is no Adjudicator specified in the Contract Agreement, the mutual consultation period stated above shall last thirty (30) days (instead of fourteen), upon expiry of which either party may move to the notification of arbitration pursuant to this GCC Clause (Settlement of Disputes).

ii. The Adjudicator shall give his or her decision in writing to both parties within thirty (30) days of the dispute being referred to the Adjudicator. If the Adjudicator has done so, and no notice of intention to commence arbitration has been given by either BMC or the Supplier within fifty-six (56) days of such reference, the decision shall become final and binding upon BMC and the Supplier. Any decision that has become final and binding shall be implemented by the parties forthwith.

b. Arbitration

i. If

1. BMC or the Supplier is dissatisfied with the Adjudicator's decision and acts before this decision has become final and binding pursuant to GCC Clause (Settlement of Disputes), or
2. the Adjudicator fails to give a decision within the allotted time from referral of the dispute pursuant to GCC Clause (Settlement of Disputes), and BMC or the Supplier acts within the following fourteen (14) days, or
3. in the absence of an Adjudicator from the Contract Agreement, the mutual consultation pursuant to GCC Clause (Settlement of Disputes) expires without resolution of the dispute and BMC or the Supplier acts within the following fourteen (14) days,

then either BMC or the Supplier may act to give notice to the other party, with a copy for information to the Adjudicator in case an Adjudicator had been involved, of its intention to commence arbitration, as provided below, as to the matter in dispute, and no arbitration in respect of this matter may be commenced unless such notice is given.

ii. Any dispute in respect of which a notice of intention to commence arbitration has been given, in accordance with GCC Clause (Settlement of Disputes), shall be finally settled by arbitration. Arbitration may be commenced prior to or after Installation of the Information System.

iii. Arbitration proceedings shall be conducted in accordance with the provisions of the Arbitration Act, 1996.

c. Notwithstanding any reference to the Adjudicator or arbitration in this clause,

i. the parties shall continue to perform their respective obligations under the Contract unless they otherwise agree;

ii. BMC shall pay the Supplier any monies due the Supplier.