MAHARASHTRA INDUSTRIAL DEVELOPMENT CORPORATION

REQUEST FOR PROPOSAL

For

Implementation of Cloud-based Enterprise Email Solution with Email Security, Data Protection and Backup Services for MIDC

Tender Notification No. : 2026_MIDC_ 1295122_1

RFP Reference No. IT Cell/E-Tender/P260503

Dated.: 15.04.2026

Issued By

General Manager (IT),

Maharashtra Industrial Development Corporation

Table of Contents

Disclaimer

The information contained in this Request for Proposal document ("**RFP**", "**tender**", or "**bid document**"), whether provided herein or subsequently provided to the bidders ("**Vendor/ Firm/ Agency**") verbally or in documentary form by the Maharashtra Industrial Development Corporation (MIDC) (hereinafter referred to as "**the Department**"), or by any of its employees or advisors, is provided to the Bidders on the terms and conditions set out in this RFP document.

This RFP is not an agreement and does not constitute an offer or invitation to any party. The purpose of this RFP is to provide the Bidders, or any other person, with information to enable them to prepare their proposal ("Bid"). This RFP includes statements that reflect various assumptions and assessments arrived at by the Department in relation to the scope of the project. Such assumptions, assessments, statements, and information contained in the RFP documents are made in consideration of the intended objectives of the project and may not be complete, accurate, or adequate. The information provided in this RFP document 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 Department accepts no responsibility for the accuracy of, or any interpretation or opinion on, the scope of the project expressed herein.

The Department, its employees, and its advisors make no representation or warranty and shall incur no liability to any person, including any Bidder, under any law, statute, rules, or regulations, or in tort, including the principles of restitution or unjust enrichment, or otherwise, for any loss, cost, expense, or damage that may arise from, or be incurred or suffered on account of, anything contained in this RFP or otherwise.

The Department also accepts no liability of any nature whatsoever, whether resulting from negligence or otherwise, howsoever caused, arising from reliance by any Bidder upon the statements contained in this RFP. The Department may, in its absolute discretion, but without being under any obligation to do so, amend or supplement the information contained in this RFP.

The issuance of this RFP document does not imply that the Department is bound to select a Bidder or to appoint the Selected Bidder (as defined hereinafter) for execution, and the Department reserves the right to reject all or any of the Bidders or Bids without assigning any reason whatsoever.

The Bidder shall bear all costs associated with or relating to the preparation and submission of its Bid, including but not limited to costs incurred for preparation, copying, postage, delivery fees, travel, consulting expenses associated with any demonstrations or presentations that may be required by the Department, and any other costs incurred in connection with or relating to its Bid. The Department shall not be liable in any manner whatsoever for such costs, regardless of the conduct or outcome of the selection process.

Invitation to the bidders

To:

Prospective Bidders

The Maharashtra Industrial Development Corporation (MIDC), Maharashtra State, Mumbai (also referred to as "The Department" or "Department" in this document) invites technical and commercial offers for the advertised tender. The bidders shall follow the procedure described on e-Tendering website (https://mahatenders.gov.in/nicgep/app) for completing their responses and for further final submissions. For further details about the e-Tendering procedure and its requirements, refer manual available on the e-Tendering website.

The tender document will be available on e-Tendering website and may be downloaded by the interested bidders. The bidders are required to submit the tender fee and EMD online on or before the last date of bid submission through e-tendering website (https://mahatenders.gov.in/nicgep/app) without which bid shall be considered incomplete & non-responsive and hence shall not be considered for evaluation. The tender fee shall be non-refundable.

The Department reserves the right to accept or reject or cancel any bid or relax any part of the tender document without assigning any reason thereof. Important information about the bid is given in Bid Control Sheet Section.

Maharashtra Industrial Development Corporation,
Maharashtra, Mumbai.

Abbreviations

Below is the list of Abbreviations used in this RFP document:

Abbreviation	Description
AD	Active Directory
AES	Advanced Encryption Standard
ATP	Advanced Threat Protection
BEC	Bidder's Evaluation Committee
BG	Bank Guarantee
BoQ	Bill of Quantities
CA	Contract Agreement
DKIM	DomainKeys Identified Mail
DLP	Data Loss Prevention
DMARC	Domain-based Message Authentication, Reporting, and Conformance
DNS	Domain Name System
DR	Disaster Recovery
EMD	Earnest Money Deposit
EOP	Exchange Online Protection
GoI	Government of India
GST	Goods and Services Tax
HoD	Head of Department
ICT	Information and Communication Technology
ISO	International Organization for Standardization
IT	Information Technology
LDAP	Lightweight Directory Access Protocol
LOA	Letter of Acceptance
LoI	Letter of Intent
MIDC	Maharashtra Industrial Development Corporation
MX	Mail Exchange
NEFT	National Electronic Funds Transfer
NOCs	No Objection Certificate

Abbreviation	Description
O&M	Operations and Maintenance
OEM	Original Equipment Manufacturer
OTP	One-Time Password
PAN	Permanent Account Number
PBG	Performance Bank Guarantee
PMC	Project Management Consultant
PQ	Pre-Qualification
QCBS	Quality cum cost-based selection
RFP	Request for Proposal
RTGS	Real Time Gross Settlement
SA	Selected Agency
SaaS	Software as a Service
SLA	Service Level Agreement
SMTP	Simple Mail Transfer Protocol
SPF	Sender Policy Framework
T&C	Terms and Conditions
TAN	The Tax Deduction and Collection Account Number
TLS	Transport Layer Security

Definitions

Sr No	Terms	Meaning
1	Bid Process	Process of selection of the successful bidder through competitive bidding and includes submission of proposals, scrutiny and evaluation of such bids as set forth in the RFP.
2	Bid / Proposal	Proposal submitted by the Bidder(s) in response to this RFP in accordance with the provisions hereof including Technical Proposal and Price Proposal along with all other documents forming part and in support thereof as specified in this RFP.
3	Completion Certificate / Go-Live Certificate	The Go-live or Completion certificate issued by the competent authority.
4	Deadline for Submission of Bids / Proposal" OR "Proposal Due Date / Bid Due Date"	Last date and time for receipt of Bids as set forth in this RFP or such other date / time as may be decided by MIDC in its sole discretion and notified by dissemination of requisite information.
5	Letter of Acceptance or LOA	The letter issued by MIDC to the Successful Bidder to undertake and execute the project in conformity with the terms and conditions (T&C) set forth in the RFP and any subsequent amendments thereof.
6	Performance Guarantee or Security Deposit	The Bank Guarantee furnished by a successful bidder as per terms and conditions of this RFP.
7	RFP or Tender	This RFP document which comprises of the following sections: Disclaimer, Scope of Work, Instruction to Bidders, Proposal Evaluation, Draft License Agreement, Service Level Agreement, Forms of Bid which include any applicable Appendix thereto.
8	Selected Bidder	The Bidder who has emerged as preferred bidder in terms of this RFP and has been issued the Work Order / Letter of Acceptance (LoA) by MIDC and awarded the work under this RFP.
9	Total Contract Value (TCV)	The total cost of a contract over its entire duration as agreed during the time of contract signing.

MAHARASHTRA INDUSTRIAL DEVELOPMENT CORPORATION

(A GOVERNMENT OF MAHARASHTRA UNDERTAKING)

Udyog Sarathi, MIDC, Mahakali Caves Road, Andheri (East), Mumbai- 400093.

E-Tender Notice No. **IT Cell/E–Tender/ P260503**

Main Portal: https://mahatender.gov.in

Online electronic bids are invited by The GM IT, IT Department, on behalf of the Maharashtra Industrial Development Corporation, from bidders with proven experience in executing similar works as mentioned below. Tender documents are available for online bid preparation and submission on the above-mentioned website from 15.04.2026 to 07.05.2026.

Sr. No.	Description	E-Tender Price	EMD	Start date & Time for online Bid Downloading	End date & Time for online Bid Submission
1	RFP for Implementation of Cloud-based Enterprise Email Solution with Email Security, Data Protection and Backup Services for MIDC	Rs. 1,20,000	Rs. 12,00,000/-	15/04/2026 05:00 PM	07/05/2026 04:00 PM

a) Additional details regarding e-tendering process are available in tender document on above portal.

b) Bidder can seek clarification through email within 7 days from the date of bid publishing

c) For any bidding portal technical related query please E-Mail- support- gmit@midcindia.org

sd/-

The General Manager,

IT Cell, MIDC Udyog Sarathi,

Mahakali Caves Road,

Mumbai-400093

MAHARASHTRA INDUSTRIAL DEVELOPMENT CORPORATION

(A GOVERNMENT OF MAHARASHTRA UNDERTAKING)

Udyog Sarathi, MIDC, Mahakali Caves Road, Andheri (East), Mumbai- 400093.

ई निविदा सूचना क्र. IT Cell/E–Tender/ P260503

संकेतस्थळ: https://mahatender.gov.in

महाराष्ट्र औद्योगिक विकास महामंडळ , यांचेसाठी खाली दर्शवलेल्या कामासाठी तत्सम प्रकारच्या कामाचा अनुभव असलेल्या कंत्राटदार यांचे कडून ई निविदा मागवत आहेत. ई निविदा कागद पत्रे दिनांक १५.०४.२०२६ ते ०७.०५.२०२६ याकालावधीत वरील संकेतस्थळावर उपलब्ध आहेत.

Sr. No.	Description	E-Tender Price	EMD	Start date & Time for online Bid Downloading	End date & Time for online Bid Submission
1	RFP for Implementation of Cloud-based Enterprise Email Solution with Email Security, Data Protection and Backup Services for MIDC	Rs. १,२०,०००	Rs. १२,००,०००/-	१५/०४/२०२६ ०५:०० PM	०७/०५/२०२६ ०४:०० PM

a) ई- **निविदा** संबंधी अतिरिक्त माहिती वरील संकेतस्थळावर उपलब्ध आहे

b) **निविदा** प्रकाशित करण्याच्या तारखेच्या ७ दिवसात कंत्राटदार ई मेल द्वारे स्पष्टीकरण मागू शकतो.

c) ई- **निविदा** प्रक्रियेसंबंधी शंका निवारण्यासाठी ई-मेल-gmit@midcindia.org

sd/-

The General Manager,

IT Cell, MIDC Udyog Sarathi,

Mahakali Caves Road,

Mumbai-400093

Bid Control Sheet

This RFP Document is being published by the MIDC for Selection of Agency for Implementing Cloud-based Enterprise Email Solution with Email Security, Data Protection and Backup Services for MIDC. Bidder agencies are advised to study this RFP document carefully before submitting their proposals in response to the RFP Notice. Submission of a proposal in response to this notice shall be deemed to have been done after careful study and examination of this document with full understanding of its terms, conditions, and implications. This RFP document is not transferable. Below are the important details:

Sr No	Information	Details
1.	Project Name/ Name of Work	Tender for Selection of Service Provider for Implementing Cloud-based Enterprise Email Solution with Email Security, Data Protection and Backup Services for MIDC * Kindly refer tender document for entire scope
2.	Tender Inviting Agency	**General Manager (IT), Maharashtra Industrial Development Corporation**
3.	Tender Reference No.	**IT Cell/ E Tender/P260503**
4.	Contact Person Name and Number for bid query	**General Manager (IT)** - Email To be sent on gmit@midcindia.org up to **24/04/2026 5:00 PM** (as per Prebid queries format provided in Annexure XII of this RFP)
5.	Availability of RFP Documents	**15/04/2026** from **05:00 PM** To **07/05/2026** up to **04:00 PM** (to be downloaded from the MahaTenders site https://mahatenders.gov.in).
6.	Period of Contract	**2 years and 2 Months + 1 Year extendable from the date of Work Order**
7.	Tender Type	Open
8.	Tender Fee (Non-Refundable)	**Rs. 1,20,000/- (Rupees One Lakh Twenty Thousand Only)** payable online on MahaTender Portal Only (Non-refundable)
9.	Bid Security (Earnest Money Deposit)	**Rs. 12,00,000/- (Rupees Twelve Lakhs Only)** payable online on MahaTender Portal Only
10.	Date of Issuance of RFP	**15/04/2026 from 05:00 PM**
11.	Last Date for Submission of Pre-Bid Queries	To be sent on gmit@midcindia.org up to **24/04/2026, 05:00 PM** (as per Prebid queries format provided in Annexure XII of this RFP in Excel)

Sr No	Information	Details
12.	Pre-Bid Meeting Time, Date and Venue	**27/04/2026, 12:00 PM (Online) ,** Meeting Link - https://midc1.webex.com/midc1/j.php?MTID=mc24375e392e2ec216b598d908ac84f1f Maharashtra Industrial Development Corporation, Udyog Sarathi, Marol Industrial Area, Mahakali Caves Road, Andheri (East), Mumbai – 400093
13.	Last date and time (deadline) for Submission of Proposal	**07/05/2026 up to 4:00 PM** @ MahaTender website.
14.	Date of Tender Opening	**08/05/2026 up to 4:00 PM** @ MahaTender website.
15.	Date, time, and venue Technical Presentations of Qualified Bidders	To be informed to the qualified bidders post Pre-qualification evaluation
16.	Place of Tender Opening	Maharashtra Industrial Development Corporation, Udyog Sarathi, Marol Industrial Area, Mahakali Caves Road, Andheri (East), Mumbai – 400093
17.	Bid validity period	180 days from the last date of bid submission
18.	Bid Security/ Earnest Money Deposit Validity Period	180 days from the last date of bid submission
19.	Currency	Currency in which the Bidders may quote the price and will receive payment is INR only.
20.	Language of Bid Submission	Proposals should be submitted in English only.

Note:

a) The above dates, time and venue may be altered by the Purchaser at its sole discretion after giving prior notice to the Bidders. The information provided in the above control Sheet is further elaborated in the subsequent sections of this RFP. Information provided in the control Sheet, and subsequent sections of this RFP are to be read in conjunction and are to be interpreted harmoniously.

b) The Bidding process shall be conducted in an online MahaTender manner. Please visit https://mahatenders.gov.in/nicgep/app for further details regarding the MahaTender process.

c) All the notification & detailed terms and conditions regarding this tender notice hereafter will be published online on web site https://mahatenders.gov.in/nicgep/app

1. Project Objective

Maharashtra Industrial Development Corporation (MIDC) seeks a qualified and experienced service provider to implement a cloud-based Enterprise Email Solution encompassing Email Security, Data Protection and Backup Solutions for Email. This unified platform should support multiple mailbox configurations with scalable storage options to meet the organization's diverse needs and form the core of MIDC's communication and collaboration infrastructure.

The solution must include advanced security features such as anti-spam, anti-malware, antivirus, and zero-day threat defense to ensure a secure email environment. Robust data protection and backup capabilities for email are critical for reliable data preservation and rapid recovery.

Seamless migration from existing systems, integration with Active Directory, and enforcement of organizational email policies, deliverability, and centralized management are essential. To boost productivity, the solution should also offer a unified collaboration ecosystem, including Single Sign-On, shared drives, video conferencing, document management, calendar sharing, and archival storage.

MIDC requires a comprehensive Endpoint Data Protection and Endpoint Backup Solution. This will secure and back up data across various endpoints, complementing the Enterprise Email Solution and ensuring holistic data security and business continuity.

The proposed solutions must be supported by 24x7 remote monitoring and support services with prompt incident response, alongside structured user adoption and training programs to maximize efficiency and user satisfaction.

By deploying these integrated solutions, MIDC aims to build a resilient, secure, and future-ready communications and data protection infrastructure that safeguards critical assets, ensures regulatory compliance, and enhances overall organizational productivity.

2. Project Background

Email is an essential communication tool for MIDC, with users spending more time on email than on telephone calls, instant messaging, or other communication channels combined. It continues to serve as the primary medium for content exchange across the department. Currently, MIDC utilizes Microsoft Outlook through multiple subscription plans, each varying in storage allocation and drive capabilities, to address diverse user requirements. After the project execution and completion of the current engagement MIDC seeks to adopt a unified and optimized email solution that aligns more effectively with the evolving needs of its workforce.

This document highlights the key considerations critical to MIDC and provides a framework to guide the selection of the most suitable email platform going forward.

A) Existing Solution:

MIDC is presently using Microsoft Office 365 for official email communication, Currently, the provision of email services to MIDC users is managed by a System Integrator (SI) appointed through a tender process for approximately 1,500 users.

Sr. No.	Description	Unit	Qty.
1	Email Solution – Exchange Online Plan -1 Type 1 Basic (50 GB)	Nos	1200
2	Email Solution – Exchange Online Plan -2 Type 2 Basic (100 GB)	Nos	200
3	Email Solution – Office 365 E1 (50 GB)	Nos	50
4	Email Solution – Office 365 E3 Type 4 Advance (100 GB)	Nos	50

3. Instructions To Bidders

3.1 General Instructions

a) The RFP document can be downloaded from the e-tendering portal at: http://mahatenders.gov.in/nicgep/app

b) Bidder agencies are advised to carefully study this RFP document and all annexures before submitting their proposals in response to the RFP notice. Submission of a proposal, along with all required data and annexures, shall be deemed to have been made after careful study and examination of this document, with full understanding of its terms, conditions, and implications. This RFP document is non-transferable.

c) The submission of the Bid shall be made online only, as per the prescribed norms. Detailed information regarding the bid submission process can be obtained from the e-tendering website: http://mahatenders.gov.in/nicgep/app

d) Bidding agencies are advised not to submit a signed and stamped copy of the RFP document along with the bid response.

e) The response to this bid document must be full and complete in all respects. Failure to furnish all required information, or submission of a proposal that is not substantially responsive to the requirements of this RFP, may result in rejection of the Bid.

f) The Bidder shall ensure that all submitted documents are clear and readable. Any unreadable document shall be treated as null and void, and only the remaining readable documents shall be considered for evaluation. The decision of the Bid Evaluation Committee in this regard shall be final and binding on all Bidders.

g) Only those Bidders who satisfy the Pre-Qualification criteria specified in Section 9 of this RFP shall be considered for further technical and commercial evaluation by the Department.

h) Submission of all forms provided in the Annexures is mandatory.

i) Possession of a valid Digital Signature Certificate (DSC) is a prerequisite for online bid submission. The Department shall not be responsible for any delay or technical issues faced by the Bidder(s) during online submission. Bidders are advised to submit their bids well in advance to avoid delays due to such issues.

j) The Bidder shall be responsible for all costs incurred in connection with participation in this bidding process, including but not limited to costs incurred for meetings, discussions, presentations, preparation and submission of the proposal, and provision of any additional information required by the Department. The Department shall not, under any circumstances, be responsible or liable for such costs, regardless of the conduct or outcome of the bidding process.

k) All materials submitted by the Bidder shall become the property of the Department and may be returned at the sole discretion of the Department.

l) All terms and conditions of this RFP and its subsequent documents shall be binding on the successful Bidder.

m) The Bidder or its representatives shall not contact Department officials for issues related to EMD submission or return, DSC functionality, the e-tendering website, or document uploads. The Department shall not be held responsible for any such issues.

3.2 Bidder's Authorized Signatory

a) The Proposal shall be accompanied by an appropriate Board Resolution or Power of Attorney in the name of the authorized signatory of the Bidder, stating that such person is duly authorized to execute documents and undertake all activities associated with the Bidder's Proposal. A copy of the same, in the format prescribed under **Annexure IV**, shall be uploaded in the relevant section / folder on the MahaTender portal.

b) Further, the response to this RFP must be submitted online after being duly signed by an authorized representative of the bidding entity.

3.3 Duration of The Project

a) The project duration shall be **2 years and 2 Months**, with a provision for extension of **one (1) additional year**, subject to the Department's regulations and the satisfactory performance of the agency, with costs remaining consistent during the extension period as per the price quoted in the commercial bid.

3.4 Consortium Conditions

a) A Bid may be submitted by a consortium of firms. The consortium shall consist of no more than two (2) parties, comprising one (1) Lead Bidder and up to one (1) consortium member. The Bidders shall not have any conflict of interest that affects the bidding process. Any Bidder found to have a conflict of interest shall be disqualified. A Bidder shall be deemed to have a conflict of interest affecting the bidding process if any constituent of one Bid is also a constituent of another Bid.

b) The Lead Bidder shall be responsible for the following:

   i. Overall project management and coordination of the Consortium Member forming part of the proposal, and for the delivery of all products and services in accordance with the terms and conditions of the Contract and as per the timelines mentioned. Taking timely review of the consortium member and brief the project status to MIDC

   ii. Supply, delivery, installation, and commissioning of all products and services submitted under the Proposal.

iii. Participation in the tender process, execution and signing of all documents related thereto, up to and including the signing of the Agreement, and fulfilment of all contractual obligations thereafter, in the event of award of the Contract.

iv. Establishment, operation, and maintenance of the complete solution for MIDC on a turnkey basis, including warranty and Comprehensive Annual Maintenance Contract (AMC) obligations.

c) Bids submitted by a consortium shall also comply with the following requirements:

i. The Lead Bidder shall be authorized to incur liabilities and receive instructions for and on behalf of all Consortium Member. The entire execution of the Contract, including invoicing and receipt of payments, shall be carried out exclusively with the Lead Bidder.

ii. The Lead Bidder shall not be a Consortium Member in any other bid submitted against this RFP.

iii. Any firm that is not a Lead Bidder for this RFP shall not participate as a Consortium Member in more than one bid submitted in response to this RFP.

iv. Internal arrangements among the Consortium Members shall be at the discretion of the Bidder. However, it shall be the sole responsibility of the Lead Bidder to ensure that all Consortium Members comply with all clauses and requirements of this RFP. Failure to ensure such compliance may result in disqualification of the Bid.

d) The validity of the Consortium Agreement entered into between the Lead Bidder and the Consortium Member shall remain effective for the entire duration of the Contract, including any extension period, as specified in this RFP. The Consortium Agreement shall be irrevocable for the said period and shall include a clause nominating the Lead Bidder to act on behalf of the Consortium Member.

e) Notwithstanding the above, both the Lead Bidder and the Consortium Member shall be jointly and severally responsible for the satisfactory execution and performance of the Contract. **An irrevocable affidavit, duly notarized and executed on appropriate non-judicial stamp paper, shall be submitted, undertaking joint and several responsibilities for all contractual obligations throughout the Contract period.**

f) The Department reserves the right to approve the Consortium Agreement and may require amendments to the agreement between the Lead Bidder and the Consortium Member, as deemed necessary.

g) The Lead Bidder shall be the single point of contact for all communications and queries related to contractual obligations under this RFP.

h) The Lead Bidder shall be fully responsible for the quality, performance, and delivery of services provided by the Consortium Member.

i) Under no circumstances shall the Department be held responsible for any issues, disputes, or concerns arising between the Lead Bidder and the Consortium Member.

j) In the event of any legal dispute or disagreement between the Lead Bidder and the Consortium Member, it shall be the sole responsibility of the Lead Bidder to ensure uninterrupted and smooth execution of all activities defined in the Scope of Work.

k) The Lead Bidder shall not, under any circumstances, replace or change the Consortium Member without the prior written consent and approval of MIDC.

3.5 Tender Form and Tender Fee

a) The tender documents are available on the Government of Maharashtra e-Tendering portal at https://mahatenders.gov.in/nicgep/app.

b) The Bidder shall fill in the Tender details in the prescribed online format and upload the required information on the portal.

c) Additionally, the Bidder shall download the Tender application form and other documents, duly fill it, and upload a scanned copy of the completed form along with all required supporting documents.

d) The blank Tender forms shall be available for download only after online payment of the Tender fee amounting to ₹1,20,000 (Rupees One Lakh Twenty Thousand only), inclusive of GST. The Tender fee shall be paid in Indian Rupees only and shall be non-refundable.

3.6 Earnest Money Deposit (EMD) and Performance Bank Guarantee (PBG)

A) Earnest Money Deposit (EMD)

a) **Earnest Money Deposit (EMD)** is Rs. 12,00,000/- (Rupees Twelve Lakhs Only) and should be deposited online as per the instructions on the e-Tendering website.

b) The EMD of all non-responsive bids shall be returned to the bidders automatically only after the Letter to Commence the Work is issued to the successful bidder or in case of cancellation of the tender by the department.

c) The EMD amount is interest-free and will be refunded to the unsuccessful bidders without any accrued interest.

d) Bidders should ensure that payment of the EMD is made prior to the last date of bid submission as per the Tender Schedule, considering the bank's clearing process lead time, to ensure seamless submission.

e) EMD shall be forfeited in the following cases:

   i. If a bidder withdraws its bid during the period of bid validity.

   ii. In the case of a successful bidder, if the bidder fails to sign the contract or furnish the Performance Bank Guarantee.

   iii. Exemption from submitting the EMD will be given to MSME agencies.

   iv. During the bid process, if a bidder indulges in any deliberate act that would jeopardize or unnecessarily delay the process of bid evaluation and finalization.

v. During the bid process, if any information is found to be wrong, manipulated, or concealed in the bid.

f) The decision of the department regarding forfeiture of the EMD and rejection of the bid shall be final and shall not be called into question under any circumstances.

g) The EMD shall be refunded to the successful bidder upon receipt of the Performance Bank Guarantee.

B) Performance Bank Guarantee (PBG)

a) The successful bidder shall, at its own expense, deposit with the Department an unconditional and irrevocable Performance Bank Guarantee (PBG) from a Scheduled / Nationalized Bank for 5% of the contract value / bid value of the successful bidder within 15 days of issue of work order and before signing of the contract. The validity of the PBG shall be six (6) months beyond the expiry of all contractual obligations. The PBG format is provided in Annexure XIII.

b) The indicative conditions in which the PBG of the successful bidder may be forfeited are:

i. Failure to commence the work within three (3) weeks from the date of issue of the Work Order.

ii. Non-compliance with the terms and conditions of the RFP.

c) The PBG may be discharged / returned by the Department upon being satisfied that there has been due performance of the obligations of the bidder under the contract. However, no interest shall be payable on the PBG.

d) The PBG of the successful bidder shall be discharged upon the bidder signing the contract, in the form and manner satisfactory to the Department, within the stipulated time.

e) In the event of the bidder being unable to service the contract for any reason whatsoever, the Department shall invoke the PBG. Notwithstanding and without prejudice to any rights of the Department under the contract, the proceeds of the PBG shall be payable to the Department as compensation for any loss resulting from the bidder's failure to fulfil its obligations under the contract, as specified in this document.

f) The Department shall notify the bidder in writing of the exercise of its right to receive such compensation within twenty (20) days, indicating the contractual obligation(s) in default.

g) The Department shall also be entitled to recover from the bidder's bills, PBG, or any other amount due to the bidder, the equivalent value of any payment made due to inadvertence, error, collusion, misconstruction, or misstatement.

h) In the event that SLA penalties become payable in an amount exceeding the balance of payments remaining under the Contract (including any extension period, if granted), the Purchaser/Client shall be entitled to recover such excess SLA penalties from the Performance Bank Guarantee (PBG). Where the remaining amount payable under the Contract and any extension period is insufficient to fully set off the SLA penalties, the shortfall may be deducted and realized from the PBG, and the lead bidder shall, upon written demand, forthwith replenish or restore the PBG to its original value within 30 days.

3.7 Pre-Bid Meeting

a) The Department will host a Pre-Bid Meeting for queries (if any) from prospective bidders. The date, time, and venue of the meeting are provided in the Bid Control Sheet. The purpose of the pre-bid meeting is to provide a forum for bidders to clarify their doubts and seek clarifications or additional information necessary for the submission of their bids.

b) All enquiries from bidders related to this bid document must be submitted to the designated contact person, as mentioned in the Bid Control Sheet, via email. Queries must be submitted strictly in the format provided in Annexure XII.

c) Queries submitted after the above-mentioned deadline, or not adhering to the prescribed format, may not be responded to. All responses to the queries (clarifications / corrigenda) shall be made available on the e-Tender website: http://mahatenders.gov.in/nicgep/app.

3.8 Submission of Bids

a) RFP response documents are to be prepared & submitted online as per instructions of e-tendering and to be uploaded on web site, digitally signed wherever necessary. The detailed step by step procedure for uploading the response documents, required RFP papers, which are available on the e-Tendering portal of Govt. of Maharashtra http://mahatenders.gov.in Bidders have to follow the instructions given on the above web site for filling up response online.

b) All the pages of the Proposal document must be **sequentially numbered and must contain the list of contents with page numbers**. Any deficiency in the documentation may result in the rejection of the Bidder's Proposal.

c) Bidders shall submit their quote including taxes applicable as on date of submission of bid.

d) The two bids system shall be followed. Technical and Financial Bids shall be uploaded separately through the e-Tendering system.

e) Late submission will not be entertained and will not be permitted by the MahaTender system.

3.9 Conflict of Interest

a) The bidder should hold Department's interest paramount, strictly avoid conflicts with other assignment(s) / job(s) or their own corporate interests, and act without any expectation/ consideration for award of any future assignment(s) from the Department. Without limitation on the generality of the foregoing, the Bidder and any of their affiliates shall be considered to have a conflict of interest and shall not be engaged, under any of the circumstances set forth below:

   i. **Conflicting Assignment / Job**: The Bidder (including their personnel) or any of its affiliates shall not be hired for any assignment/job that, by its nature, may conflict with the Department's project.

   ii. **Conflicting relationships:** The Bidder (including their personnel) that have a business or

family relationship with a member of Department's staff who is directly or indirectly involved in any part of implementation of the proposed solution may not be awarded a contract, unless the conflict stemming from such a relationship has been resolved in a manner acceptable to the Department throughout the selection process and the execution of the contract.

iii. **Hiring of Employees**: During the term of agreement, Bidder will not appoint any staff of the Department either as an employee or a consultant. The same would apply to the Department as well.

b) The Bidder has an obligation to disclose any situation of actual or potential conflict that impacts on their capacity to serve in the best interests of the Department, or that may reasonably be perceived as having this effect. If the Bidder fails to disclose such conflicts of interest and if the Department comes to know about any such situation at any time, then the Department reserves the right to disqualify the Bidder during the bidding process or to terminate their contract during execution of the assignment.

c) This contract should not impact on any of the existing relationships of the Department with any of its clients / bidders / suppliers / customers.

3.10 Amendment of RFP Document

a) At any time before the deadline for submission of bids, the Department may, for any reason, whether at its own initiative or in response to a clarification requested by a prospective Bidder, modify the RFP document by amendment. All the amendments made in the document would be informed to all the participating agencies through mail or as a corrigendum published on E-Tender Site (https://mahatenders.gov.in/nicgep/app)

b) Any modification to the RFP document shall be prepared by the Department as an addendum/corrigendum. The addendum/corrigendum will be hosted on E-Tender Site.

c) The bidders are advised to periodically visit the e-Tender Site (https://mahatenders.gov.in/nicgep/app) for checking necessary updates regarding any further corrigendum / addendum / notice published with respect to this tender. The Department also reserves the right to amend the dates mentioned in this RFP for bid process.

d) All such supplements shall be part of the RFP, and the bidders shall submit their bids on that basis.

3.11 Right To Reject Any Proposal

a) Notwithstanding anything contained in this RFP, the Department reserves the right to accept or reject any proposal and to annul the selection process and reject all proposals, at any time without any liability or any obligation for such acceptance, rejection, or annulment, and without assigning any reasons, therefore.

b) The Department reserves the right to reject any Proposal if

i. At any time, a material misrepresentation is made or discovered, or

ii. The Bidder does not provide, within the time specified by the Department, the supplemental

information sought by the Department for evaluation of the Proposal.

iii. Any act or omission of the Bidder results in violation of or noncompliance with this RFP document or any Applicable Laws

iv. RFP response not submitted as per the format specified in the RFP document.

v. RFP response received without the Letter of Authorization / Power of Attorneys

vi. RFP response found to suppress the details.

vii. RFP response submitted with incomplete information/illegible documents, subjective, conditional and/or partial offer is submitted.

viii. RFP response submitted without the documents requested in the checklist.

ix. RFP response non-compliant with any of the clauses stipulated in the RFP.

x. RFP response with lesser validity period than as stipulated

xi. RFP response with party to multiple bids by a bidder (as lead bidder or consortium partner).

c) Misrepresentation/ improper response by the Bidder may lead to the disqualification. If such disqualification / rejection occurs after the Proposals have been opened and the highest-ranking Bidder gets disqualified / rejected, then the Department reserves the right to consider the next best Bidder or take any other measure as may be deemed fit in the sole discretion of the Department, including annulment of the Selection Process.

d) The Department reserves the right to verify all statements, information and documents submitted by the Bidder in response to the RFP document and the Bidder shall, when so required by the Department, make available all such information, evidence and documents as may be necessary for such verification. Any such verification, or lack of such verification, by the Department shall not relieve the Bidder of its obligations or liabilities hereunder nor will it affect any rights of the Department thereunder.

e) No response can be modified by the Bidder, after the closing date and time for submission of bid. If date of submission is extended due to some reasons, modification in RFP is possible till extended period provided RFP has not been opened.

f) Withdrawal of RFP response is not permissible after its submission. If the RFP response is withdrawn before the validity period, the EMD will stand forfeited.

3.12 Bid Validity

a) The offer submitted by the Bidders should be valid for minimum period of 180 days from the date of submission of the Bid. On completion of the validity period, unless the Bidder withdraws his bid in writing, bid validity shall be deemed to be extended until such time that the contract is awarded to successful Bidder or Bidder formally (in writing) withdraws his bid.

3.13 Language of Bids

a) The Bids prepared by the Bidder and all correspondence and documents relating to the bids exchanged by the Bidder and the Department, shall be written in English language, provided that any printed literature furnished by the Bidder in another language shall be accompanied by an English translation in which case, for purposes of interpretation of the bid, the English translation shall govern.

b) If any supporting documents submitted are in any language other than English, translation of the same in English language is to be duly attested by the bidder.

3.14 Department's Rights to Terminate the Process.

a) The Department may terminate the RFP process at any time without assigning any reason. The Department makes no commitments, express or implies that this process will result in a business transaction with anyone.

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

3.15 Evaluation Process

a) The evaluation process of the bid proposed to be adopted by the Department is indicated in this section. The Department shall appoint a Bid Evaluation Committee (BEC) to scrutinize and evaluate the technical and commercial bids received. The BEC will examine the bids to determine whether they are complete, responsive and whether the bid format conforms to the bid requirements. The department may waive any informality or non-conformity in a bid which does not constitute a material deviation. There should be no mention of bid prices in any part of the bid other than the Commercial Bid. Any attempt by a bidder to influence the bid evaluation process may result in the rejection of Bid.

b) In the first stage Technical Bids will be opened in the presence of the Bidder's representatives who may be present at the opening time.

c) In the second stage Financial Bids will be opened in the presence of the Bidder's representatives who may be present at the opening time.

d) All the bidding entities should fulfil the Pre-Qualification (PQ) Criteria. Only entities fulfilling the PQ Criteria will be considered for the technical and commercial evaluation. The bid will be two stage process and based on **Quality and Cost based System (QCBS) of evaluation.**

e) After PQ, the first stage will be Technical Evaluation (TE) of the proposal based on the technical criteria and second stage will be Financial Evaluation (FE) based on the financial quote by the bidder.

The final evaluation will be based on the weightage given to the Technical and Financial performance by the bidder as detailed in this section.

f) At the end of the evaluation of technical proposal of the bidders, based on the performance on various technical parameters, bidders will be allotted Marks. After the Technical evaluation, the companies scoring more than the minimum Marks required will move to second stage and their financial proposal will be evaluated. Then the bidders will be allotted Marks based on their financial proposal. The Technical and Financial Marks will then be added to get the Overall Marks.

g) The Evaluation Process is detailed out in subsequent sections of this RFP.

3.16 Notifications of Award and Signing of Contract

a) The QCBS method is applicable for evaluation of proposals after successful Pre-Qualification. Prior to the expiration of the period of bid validity, the MIDC will notify the successful Bidder that its bid has been accepted. Successful Bidder shall submit the performance Bank Guarantee after the contract is awarded and before execution of the contract. The notification of award will constitute the formation of the Contract. Upon successful Bidder's, furnishing of Performance Bank Guarantee the department may notify each unsuccessful Bidder. Successful Bidder shall pay PBG (Performance Bank Guarantee) within 15 working days of notification of award.

b) The Department shall facilitate signing the contract within the period of 15 days of the notification of award. However, it is to be noted that the date of commencement of the project and all contractual obligations shall commence from the date of issuance of Work Order. All reference timelines shall be considered beginning from the date of issuance of the Work Order; subject to changes made by MIDC.

c) The general process to be followed shall be as under:

   i. Declaration of results on the MahaTender portal. **(D)**
   ii. Issuance of the Letter of Intent (LoI) to the successful bidder by the Department **(D + 2 days).**
   iii. Submission of the Letter of Acceptance (LoA) against the issued LoI by the successful bidder within the stipulated timeline **(D + 5 days).**
   iv. Issuance of the Work Order to the successful bidder by the Department **T = (D + 7 days).**
   v. Submission of the Letter of Acceptance against the issued Work Order by the successful bidder within the stipulated timeline **(T + 10 days).**
   vi. Submission of the Performance Bank Guarantee (PBG) by the bidder **(T + 15 days).**
   vii. Signing of the Contract **(T + 15 days)**

3.17 Post Signing of Contract

a) During the project duration, the successful bidder shall, whenever required by MIDC officials, visit the MIDC Office located at Andheri, Mumbai, at its own cost.

3.18 Acceptance Conditions

a) The bidder shall confirm unconditional acceptance of full responsibility for completion of the work and for execution of the Scope of Work under this RFP. Such confirmation shall be submitted as part of the Technical Bid. The bidder shall also be the sole point of contact for all purposes related to the contract.

b) The bidder shall not be involved in any litigation that may adversely affect or compromise the delivery of services as required under this contract. If, at any stage of the tendering process or during the currency of the contract, any suppression or falsification of such information is brought to the notice of MIDC, MIDC shall have the right to reject the bid or terminate the contract without any compensation to the bidder.

3.19 Force Majeure

a) Force Majeure is herein defined as any cause which is beyond the control of the selected Bidder or MIDC which they could not foresee or with a reasonable amount of diligence could not have foreseen and which substantially affects the performance of the contract, such as:

   i. Natural phenomenon, including but not limited to floods, droughts, earthquakes, and epidemics disruption caused due to Pandemic / Lockdown situation much graver than current situation.

   ii. Acts of any government, including but not limited to war, declared or undeclared priorities, quarantines and embargos.

   iii. Terrorist attack, public unrest in work area provided either party shall within 10 days from occurrence of such a cause, notifies the other in writing of such causes. The Bidder or MIDC shall not be liable for delay in performing his/her obligations resulting from any force majeure cause as referred to and/or defined above.

   iv. Any delay beyond 30 days shall lead to termination of contract by parties and all obligations expressed quantitatively shall be calculated as on date of termination. Notwithstanding this, provisions relating to indemnity and confidentiality survive termination of the contract.

3.20 Failure to Agree with Terms & Conditions of Bid Document

a) This RFP Document is confidential, and the Bidder shall ensure that anything contained in this RFP document shall not be disclosed in any manner, whatsoever. Failure of the bidder to agree with the Terms & Conditions of the Bid Document shall constitute sufficient grounds for the annulment of the award of contract, in such event the contract may be awarded to the next most responsive bidder(s).

3.21 Indemnity

a) The successful bidder shall indemnify, protect, and save the Department against all claims, losses, costs, costs, damages, expenses, action suits and other proceedings, resulting from infringement of any patent, trademarks, copyrights etc. rendered by the bidder.
b) Bidder shall agree to be responsible for managing the activities of its personnel or the personnel of its partner/subsidiary members (if any) and shall be accountable for both.
c) Bidder shall agree to hold the Department, its employees, agents, representatives, and administrators fully indemnified and harmless against loss or liability, claims actions or proceedings, if any, that may arise from whatsoever nature caused to the Department through the action of its employees, agents, OEM Personnel etc.
d) Bidder shall not disclose any citizen information (email id, phone number, address, property id, payment details etc.)

3.22 Confidentiality

a) Information relating to the examination, evaluation, comparison, and post qualification of bids, and recommendation of contract award, shall not be disclosed to bidders or any other persons not officially concerned with such process until publication of the Contract award.
b) Any attempt by a bidder to influence the tendering authority or other officials in the examination, evaluation, comparison, and post qualification of the bids or Contract award decisions may result in the rejection of his bid.

3.23 Contract Termination

a) Department may, without prejudice to any other remedy under this Contract and applicable law, reserves the right to terminate for breach of contract by providing a written notice of 30 days stating the reason for default to the Agency and terminate the contract either in whole or in part:
    i. If the Agency fails to deliver any or all the project requirements / operationalization / Operational Acceptance of project within the time frame specified in the contract; or
    ii. If the Agency fails to perform any other obligation(s) under the contract.
    iii. Prior to providing a notice of termination to the Selected Agency, department shall provide the Selected Agency with a written notice of 15 days instructing the selected Agency to cure any breach/ default of the Contract, if department is of the view that the breach may be rectified.
    iv. On failure of the Selected Agency to rectify such breach within 15 days, department may terminate the contract by providing a written notice of 30 days to the Agency, provided that such termination will not prejudice or affect any right of action or remedy which has accrued or will accrue thereafter to department. In such an event the Agency shall be liable for penalty imposed by department.

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

vi. **Termination for insolvency**: The Department may at any time terminate the contract by giving 30 days' written notice to the selected Bidder if the latter becomes bankrupt or otherwise insolvent. In this event, termination will be without compensation to the selected Bidder, provided that such termination will not prejudice or affect any right of action or remedy which has accrued or will accrue thereafter to the Department.

vii. Default is said to have occurred:

- If the selected Bidder fails to deliver any or all contracted services as per service standards specified in the Contract.
- If the selected Bidder fails to perform any other obligation(s) under the Contract
- If the selected Bidder in the judgment of the Department has engaged in corrupt or fraudulent practices in competing for or in executing the Contract
- If the agency, in either of the above circumstances, does not take remedial steps within a period of 30 days after receiving the default notice from the Department may terminate the contract / work order in whole or in part.

viii. In situation of insolvency of the selected bidder, the Department shall recover the due funds from bidder as per the timelines defined in section .

3.24 Applicable Law & Legal Jurisdiction

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

b) Attachments to the Agreement can be following documents:

i. Scope of Services for the Agency
ii. Detailed Commercial proposal of the Agency accepted by department.
iii. Corrigendum Document published if any by the department, after the Bid Document for this work.
iv. RFP Document of department for this work

v. Letter of Intent (LoI) issued by department to the successful bidder.
vi. The successful bidder's "Technical Proposal" and "Commercial Proposal" submitted in response to the Bid Document

3.25 Fraud and Corruption

a) Department requires that Agency observes the highest standards of ethics during the execution of the contract. In pursuance of this policy, department defines, for the purpose of this provision, the terms set forth as follows:
   i. "Corrupt practice" means the offering, giving, receiving, or soliciting of anything of value to influence the action of department in contract executions.
   ii. "Fraudulent practice" means a misrepresentation of facts, to influence a procurement process or the execution of a contract, to department, and includes collusive practice among bidders (prior to or after bid submission) designed to establish bid prices at artificially high or non-competitive levels and to deprive department of the benefits of free and open competition.
   iii. "Undesirable practice" means: establishing contact with any person connected with or employed or engaged by department with the objective of canvassing, lobbying or in any manner influencing or attempting to influence the Selection Process; or Having a Conflict of Interest
   iv. "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.
   v. "Coercive Practices" means harming or threatening to harm, directly or indirectly, persons or their property to influence their participation in the execution of contract.
b) If it is noticed that the Agency has indulged into the Corrupt / Fraudulent / Undesirable / Coercive practices (as decided by a court or competent authority with appropriate jurisdiction), it will be sufficient ground for Department to terminate the contract and initiate blacklisting of the bidder.

3.26 Maharashtra Stamp Act 2015

a) The Agency shall pay Stamp Duty on agreement as per provision of Maharashtra Stamp Act 2015 as below:
   i. Where the amount or value set forth in such contract does not exceed Rupees Five Lakh →Five hundred Rupees
   ii. Where the amount or value set forth in such contract exceeds Rupees Five Lakh →Five Hundred plus 0.3% of the amount above Rupees Ten Lakh subject to maximum of Rupees Twenty-Five Lakhs.

3.27 Goods and Service Tax (GST)

a) At the time of payment of invoices, MIDC shall retain the GST amount as a deposit and pay it later to the Agency. However, the amount shall be reimbursed or paid to the Agency upon submission of proof of payment of the GST, after it is reflected in GSTR-1 on the GSTIN portal.

3.28 Dispute Resolution Mechanism

a) The Successful Agency and the MIDC shall endeavor their best to amicably settle all disputes arising out of or in connection with the Contract in the following manner:
b) The Party raising a dispute shall address to the other Party, a notice requesting an amicable settlement of the dispute within seven (7) days of receipt of the notice.
c) The matter will be referred for dispute resolution between MIDC and the Authorized Signatory of the Software Development Agency. The matter shall then be resolved between them, and the agreed course of action documented within a further period of 15 days.
d) In case any dispute between the Parties, does not settle in the manner as mentioned above, the same may be resolved exclusively by arbitration and such dispute may be submitted by either party for arbitration within 20 days of the failure of negotiations. Arbitration shall be held in Mumbai and conducted in accordance with the provisions of Arbitration and Conciliation Act,1996.
e) The arbitration award shall be final, conclusive and binding upon the Parties and judgment may be entered thereon, upon the application of either party to a court of competent jurisdiction. Each Party shall bear the cost of preparing and presenting its case, and the cost of arbitration, including fees and expenses of the arbitrators, shall be shared equally by the Parties unless the award otherwise provides.
f) The Successful Agency shall not be entitled to suspend the Service/s or the completion of the job, pending resolution of any dispute between the Parties and shall continue to render the Service/s in accordance with the provisions of the Contract/Agreement notwithstanding the existence of any dispute between the Parties or the subsistence of any arbitration or other proceedings.

3.29 Rejection Criteria

a) Besides other conditions and terms highlighted in the tender document, bids may be rejected under following circumstances:

b) General Rejection Criteria

i. Bids received through Telex /Telegraphic / Fax / E-Mail except wherever required.
ii. Bids which do not confirm unconditional validity of the bid as prescribed in the RFP.
iii. If the information provided by the Bidder is found to be incorrect / misleading at any stage / time during the Tendering Process
iv. Any effort on the part of a Bidder to influence the MIDC's bid evaluation, bid comparison or contract award decisions.

v. Bids received by the MIDC after the last date for receipt of bids prescribed by the MIDC.
vi. Does not include requisite documents.
vii. Bids without signature of person(s) duly authorized on required pages of the bid.
viii. Bids without power of authorization and any other document consisting of adequate proof of the ability of the signatory to bind the Bidder.

c) Technical Rejection Criteria

i. Technical Bid containing financial details.
ii. Revelation of Prices in any form or by any reason before opening the Financial Bid
iii. Failure to furnish all information required by the RFP Document or submission of a bid not substantially responsive to the RFP Document in every respect.
iv. Bidders not quoting for the complete scope of Work as indicated in the RFP documents, addendum (if any) and any subsequent information given to the Bidder.
v. Bidders not complying with the Technical and General Terms and conditions as stated in the RFP Documents
vi. The Bidder not confirming unconditional acceptance of full responsibility of providing services if the bid does not conform to the timelines indicated in the bid.

d) Financial Rejection Criteria

i. Incomplete Price Bid
ii. If a firm quotes NIL charges / consideration, the bid shall be treated as unresponsive and will not be considered.
iii. Price Bids that do not conform to the BOQ price format.
iv. If there is an arithmetic discrepancy in the financial bid calculations the MIDC shall rectify the same. If the Bidder does not accept the correction of the errors, its bid may be rejected.

31.30 Risk Purchase Clause

a) In the event Bidder fails to execute the project as per the stipulated timeline, or as per the directions given by MIDC from time to time, MIDC reserves the right to procure similar services from the next eligible OEM or from alternate sources at the cost of the Bidder. Before taking such a decision, MIDC shall serve a notice period of 15 days to the Bidder. The 15 days' notice period shall be considered as the 'Cure Period' to facilitate the Bidder to cure the breach. The provision for Risk Purchase shall be evoked in the event the Bidder fails to correct the breach within the 'Cure Period'. Bidder liability in such case would not be higher than 50% of the total contract value.

31.31 Limitation of Liability towards MIDC

a) The Bidder's liability under the resultant Agreement shall be determined as per the Law in force for the time being. The bidder shall be liable to MIDC for loss or damage occurred or caused or likely to occur on account of any act of omission on the part of the bidder and its employees, including loss

caused to MIDC on account of defect in goods or deficiency in services on the part of bidder or his agents or any person / persons claiming through or under said bidder. However, such liability of bidder shall not exceed the total value of the Agreement.

b) Bidder's aggregate liability in connection with obligations undertaken as a part of this contract regardless of the form or nature of the action giving rise to such liability, shall be at actual and limited to the amount paid by MIDC for:
   i. The particular hardware /software; or
   ii. Services provided during the twelve (12) months immediately preceding the date of the claim; that in each case is the subject of the claim.

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

31.32 Data Ownership

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

b) The ownership of the application for the three sub-systems and the data shall rest with MIDC.

31.33 Non-Applicability of Milestone-Based Payments (for Migration) in Case of Same OEM Selection

a) In the event that the Original Equipment Manufacturer (OEM) proposed in the Bid is the same OEM as that already engaged or otherwise selected under the Contract, Milestone-based payment structure against Migration costs and corresponding implementation timelines linked to such milestones, as may have been indicated in the Bid or standard documentation, shall not be applicable or considered for this engagement. In such a case, the payment terms and timelines shall be governed exclusively by the payment schedule and timelines expressly stipulated in this Contract, and no separate or additional milestone payments shall be admissible on account of the selection of the same OEM.

31.34 Exit Management / Transition-Out Services

A) Exit Management

a) Continuity and performance of the services at all times, including during the term of the agreement and post-expiry of the agreement, is a critical requirement of MIDC. It shall be the prime responsibility of the Lead Bidder during the exit management period to ensure that no facility or service is affected or degraded. Further, the Lead Bidder shall be responsible for all

activities required for training and knowledge transfer to MIDC or MIDC's representative agency.

b) The exit management period shall commence, in the case of expiry of the contract, at least three (3) months prior to the date of contract expiry, or, in the case of termination of the contract, from the date on which the notice of termination is issued to the Lead Bidder. The exit management period shall end on the date agreed upon by MIDC or three (3) months from the commencement of the exit management period, whichever is earlier.

c) At the end of the contract period or upon termination of the contract, the Lead Bidder shall provide the necessary handholding and transition support to ensure continuity and performance of the services to the complete satisfaction of MIDC.

B) Exit Management Plan

a) The Lead Bidder shall provide MIDC with a recommended "Exit Management Standard Operating Procedure (SOP)" within ninety (90) days from the date of signing of the contract. The Exit Management SOP shall, at a minimum, address exit management aspects relating to the SLA as a whole, Project Implementation, Operations and Management SLA, and the defined Scope of Work.

b) The Lead Bidder shall provide all necessary support to MIDC for the transfer of data and/or applications during the exit management phase, in accordance with applicable guidelines.

c) The Exit Management Plan shall include, but not be limited to, the following:

   i. A detailed program for the transfer process to be undertaken in coordination with a replacement vendor, including mechanisms to ensure uninterrupted service delivery throughout the transition period or until cessation of services, and the management structure to be adopted during the transfer.

   ii. Communication plans for bidders, staff, suppliers, customers, and relevant third parties, as necessary, to avoid any material or adverse impact on the project operations during the transition.

   iii. Plans for providing contingent support for implementation of the IT Infrastructure Solution for a reasonable period, with a minimum duration of one (1) month after the transfer.

   iv. The transition methodology, including clearly defined roles and responsibilities of both parties for handover and takeover of regular project activities and support systems.

   v. A proposal for the necessary setup or institutional structure required at the MIDC level to effectively maintain the project after contract expiry.

   vi. Training and handholding of MIDC staff or designated officers for maintenance and operation of the project after contract expiry.

d) MIDC shall review and approve the Exit Management Plan after necessary consultations and shall thereafter initiate preparations for transition.

C) Exit Management Services

a) The Lead Bidder shall be responsible for copying and transferring all data, scripts, software, virtual machine images, and related artifacts to MIDC-supplied, industry-standard media to enable mirroring, replication, or migration.

b) The Lead Bidder shall retain all data and database copies for a minimum period of ninety (90) days after expiry or termination of the contract and shall ensure that no data is deleted during this period without prior written confirmation from MIDC.

c) The format of the data transmitted from the Lead Bidder to MIDC shall, wherever feasible, adhere to standard and open data formats to ensure portability. The Lead Bidder shall ensure that all virtual machine formats are compliant with applicable standards, enabling MIDC to migrate, export, and use the data independently across platforms.

d) The Lead Bidder shall ensure that all documentation required by MIDC for a smooth transition, including configuration documents and operational manuals, is complete, accurate, and kept up to date. All such documentation shall be handed over to MIDC at regular intervals and during the exit management process.

e) Upon completion of the exit management process, all MIDC data and content shall be securely removed from the Lead Bidder's systems to ensure that such data is not recoverable, subject to confirmation by MIDC.

f) The Lead Bidder shall decommission and withdraw all hardware and software components deployed under the contract upon completion or termination of the contract and shall formally close the project.

g) At any time during the exit management period, the Lead Bidder shall provide MIDC and/or any replacement vendor with access to all relevant information required to prepare an inventory of virtual machines, assets (hardware and software, active and passive), documentation, manuals, catalogues, archived data, live data, policy documents, and any other material related to the implementation of the IT Infrastructure Solution for MIDC.

31.35 Miscellaneous

A) Standards of Performance

a) The bidder shall provide the services and perform its obligations under the contract with due diligence, efficiency, and professionalism, in accordance with generally accepted professional standards and practices.

b) The bidder shall at all times act in good faith in respect of any matter relating to this contract. The bidder shall comply with all applicable provisions of laws, acts, rules, regulations, standing orders, and information technology standards as prevalent in the country.

c) The bidder shall also conform to the standards and guidelines prescribed by the Government of Maharashtra and/or the Government of India from time to time. Such standards and guidelines shall be shared with the bidder by MIDC upon signing of the contract.

B) Care to be taken while working at MIDC Office

a) The bidder shall comply with all instructions issued by the concerned competent authority from time to time for carrying out the work at designated locations.
b) The bidder shall ensure that no damage is caused to any public or private property during execution of the work.
c) In the event of any such damage, the bidder shall immediately notify the concerned authority and MIDC in writing and shall bear and pay all costs required for rectification or restoration of such damage.
d) The bidder shall ensure that its employees and/or representatives do not breach the privacy of any citizen or establishment during the execution or maintenance of the project.

C) Independent Contractor

a) Nothing in this Agreement shall be construed as creating or implying any partnership, joint venture, or employer–employee relationship between the Parties.
b) Except as expressly provided in this Agreement, nothing herein shall be deemed to constitute either Party as an agent of the other, or to authorize either Party to
    i. Incur any expense on behalf of the other Party,
    ii. Enter into any engagement or make any representation or warranty on behalf of the other Party,
    iii. Pledge the credit of, or otherwise bind or obligate, the other Party, or
    iv. Commit the other Party in any manner whatsoever, in each case without the prior written consent of the other Party.

D) Waiver

a) Any waiver of any provision of this Agreement or of any breach thereof must be made in writing and signed by a duly authorized official of the Party granting such waiver.
b) No such waiver shall be construed as a waiver of any subsequent breach of the same provision or of any other provision of this Agreement.

E) Notices

a) Any notice or other document to be given by either Party under this Agreement shall be given in writing, either in person or by prepaid registered/recorded delivery post.
b) Any such notice or document shall be addressed to the other Party at its principal or registered

office address.

F) Personnel / Employees

a) Personnel/employees assigned by the bidder to perform the services shall be employees of the bidder and/or its subcontractors, and under no circumstances shall such personnel be considered employees of MIDC. The bidder shall have sole responsibility for the supervision and control of its personnel and for payment of their entire compensation, including salaries, statutory deductions, withholding of income tax and social security contributions, workers' compensation, employee and disability benefits, and all other employee related obligations, in accordance with applicable laws from time to time. MIDC shall not be responsible for any matters relating to the bidder's personnel.

b) The bidder shall use its best efforts to ensure that sufficient personnel are deployed to perform the services and that such personnel possess the appropriate qualifications and experience. MIDC or its nominated agencies shall have the right to require the removal or replacement of any bidder personnel engaged in the performance of services under this Agreement. In the event MIDC requests such replacement, the substitution shall be carried out in accordance with a mutually agreed schedule and subject to clearance by MIDC or its nominated agencies based on profile review and, where required, personal interaction, in line with the defined SLAs. The bidder shall deploy a suitably qualified project team, and MIDC shall have the right to require changes to the team, as necessary.

c) Senior management of the bidder (Regional Head / Vice President level or equivalent) shall be involved in project monitoring and shall attend project review meetings at least once every quarter.

d) Each Party shall be responsible for the performance of its respective obligations under this Agreement and shall be liable for the acts and omissions of its employees, agents, and authorized representatives in connection therewith.

G) Variations & Further Assurance

a) No amendment, variation, or other change to this Agreement or the SLAs shall be valid unless made in writing and signed by the duly authorized representatives of the Parties to this Agreement.

b) Each Party to this Agreement or the SLAs agrees to enter into or execute, without limitation, any further agreement, document, consent, or waiver, and to do all such acts and things as may be reasonably required to complete, perform, and give effect to the obligations set out in this Agreement or the SLAs.

c) The Department reserves the right to increase or decrease the quantity to be ordered by up to twenty-five percent (25%) of the bid quantity at the time of placement of the contract. The Department also reserves the right to increase the ordered quantity by up to twenty-five percent (25%) of the contracted quantity during the currency of the contract, at the contracted rates. Bidders shall be bound to accept such variations accordingly.

d) It is hereby clarified that any change of control exceeding twenty-five percent (25%) of the value of this project shall be considered as the subject matter of a separate bid process and a separate contract. It is further clarified that the twenty-five percent (25%) value of the project referred to herein shall be calculated on the basis of the bid value submitted by the successful bidder and duly accepted and approved by the Department.

H) Severability & Waiver

a) If any provision of this Agreement or the SLAs, or any part thereof, is held by any court or administrative body of competent jurisdiction to be illegal, invalid, or unenforceable, such illegality, invalidity, or unenforceability shall not affect the remaining provisions of this Agreement or the SLAs, which shall continue in full force and effect. The relevant Parties shall negotiate in good faith to substitute such illegal, invalid, or unenforceable provision with a valid and enforceable provision that achieves, to the greatest extent possible, the economic, legal, and commercial objectives of the original provision, within seven (7) working days.

b) No failure or delay by either Party in exercising or enforcing any right, remedy, or provision under this Agreement or the SLAs shall operate as a waiver thereof, nor shall any single or partial exercise or enforcement of any such right, remedy, or provision preclude any other or further exercise or enforcement of the same or any other right, remedy, or provision.

I) Survivability

a) The termination or expiry of this Agreement or the SLAs, for any reason whatsoever, shall not affect or prejudice any provisions of this Agreement or the SLAs, or the rights and obligations of the Parties thereunder, which are expressly stated or by implication intended to survive or continue in effect after such termination or expiry.

4. Scope of Work

4.1 Key Highlights of Scope of Work

Sr No	Scope of Work	Summary
1	**Email as Service (Basic) – 1200 users**	● Up to 50 GB primary mailbox + Archival Space ● Compliance Archiving & advanced content discovery ● Email protection- Anti Spam and Anti Malware ● Full synchronization across mobile devices, tablets & web browsers. • Collaboration Platform for chat, calls, and meetings with recording.
2	**Email as Service (Standard) - 200 users**	● Up to 100 GB primary mailbox + Archival Space ● In-Place Hold & Litigation Hold: Preserves mailbox data for compliance or legal reasons. ● Auto-expanding archiving and management of inactive mailboxes. ● Email protection- Anti Spam and Anti Malware ● Full synchronization across mobile devices, tablets & web browsers. • Collaboration Platform for chat, calls, and meetings with recording.
3	**Email Collaborative Plan (Entry-Level) - 100 users**	● Up to 50 GB primary mailbox+ Archival Space ● Up to 1 TB cloud storage per user ● Compliance Archiving & advanced content discovery ● AI Features- inbuilt Generative AI tool with limited AI functionalities for users with Enterprise Data Protection. ● Email protection- Anti Spam and Anti Malware ● Collaboration & productivity enhancement features including web versions of office apps (word processing, spreadsheets, presentations), chat, meetings • Collaboration Platform for chat, calls, and meetings with recording.
4	**Email Collaborative Plan (Advanced) - 100 users**	● Up to 100 GB primary mailbox + Archival Space ● Up to 1 TB cloud storage per user ● Compliance Archiving, advanced content discovery, Legal hold ● Email Security features – Anti Spam and Anti Malware ● AI Features- inbuilt Generative AI tool with limited AI functionalities for users with Enterprise Data Protection.

Sr No	Scope of Work	Summary
		• Collaboration & productivity enhancement features including web versions of office apps (word processing, spreadsheets, presentations), chat, meetings • Collaboration Platform for chat, calls, and meetings with recording.
5	**Email Security**	• Protection for 1500 users against malware, phishing, spoofing, advanced persistent threats (APT), zero-day attacks, and spam filtering • Domain reputation management and real-time threat monitoring.
6	**Data Protection – Email**	• Comprehensive data privacy and protection for 1500 email users including data encryption at rest and in transit, retention for audit purposes, secure access controls, and compliance with regulatory requirements.
7	**Data Protection – Endpoint**	• Protection for 2000 endpoint devices with data loss prevention to protect endpoint data integrity.
8	**Backup – Endpoint (20 TB)**	• Backup and recovery solutions for 2000 endpoints with a total storage capacity of 20 TB, including automated backups, secure storage, quick restore capabilities, and periodic backup validation.
9	**Backup – Email**	• Backup services for 1500 email users ensuring complete mailbox backup, including emails, contacts, calendar entries, archives, and encrypted mail with zero data loss and restoration capability.

4.2 Detailed Scope of Work

a) In view of the upcoming renewal and the evolving requirements related to cybersecurity, data protection, and regulatory compliance, MIDC intends to implement a cloud-based (SaaS), enterprise-grade Email Solution along with integrated Email Security, Data Protection, and Backup Services.

b) Due to the increasing incidence of cybersecurity threats such as phishing, malware, ransomware, and zero-day attacks, it has become essential for MIDC to implement a comprehensive and robust protection mechanism for its email systems and end-user data. The proposed solution is expected to strengthen MIDC's security posture and reduce risks associated with data breaches and service disruptions.

c) MIDC intends to migrate its existing email solution to a secure, cloud-based SaaS email platform.

d) The scope of work shall include, but shall not be limited to, Provision of the proposed email solution, Migration of existing email data to the proposed email service provider, Supply, installation, configuration, and maintenance of the proposed Email Security, Data Loss Prevention (DLP), and Backup solution.

The detailed scope includes but not limited to below components as mentioned in RFP:

A) Enterprise Email Solution

a) Provision of enterprise-grade email solution with scalable architecture as per industry best practice.

b) Multi-device access including web, desktop, and mobile clients with synchronization

c) Collaboration features such as shared calendars, contacts, distribution lists, chat, and task management

d) The email solution should provide logs for CERT-In audit compliances if required.

B) Email Security

a) Advanced threat protection including spam, phishing, and malware detection

b) Email encryption for data in transit and at rest

c) Role-based access control with granular permissions and audit logging

d) Support for multi-factor authentication and password-less authentication

C) Data Protection (Email & Endpoint)

a) Data Loss Prevention (DLP) through policy-based controls to prevent unauthorized sharing of sensitive data.

b) Endpoint compliance checks and device posture validation prior to access

c) Audit logs, breach detection, and reporting mechanisms to meet compliance requirements

D) Backup Solutions (Email & Endpoint)

a) Automated and scheduled backups with configurable retention policies
b) Granular restore capability for individual emails, files, or full systems
c) Monitoring and reporting dashboards for backup status, recovery validation, and compliance audits

4.3 Email Solution (For 1500 Users)

a) The Service Provider shall provide a cloud-based, scalable, enterprise-grade email solution ensuring compliance with data sovereignty laws and providing high availability and have a provision to keep a copy of data in India as and when required.

4.3.1 Provisioning of Email Mailboxes (with Quantities)

Mailbox Type	Storage	Quantity
Type 1 Basic	50 GB	1200 Users
Type 2 Basic	100 GB	100 Users
Type 3 Advance	50 GB	100 Users
Type 4 Advance	100 GB	100 Users

a) Each mailbox tier must include:
   i. Defined storage allocation per mailbox type.
   ii. High availability, fault-tolerance, and the data in transit and rest should be encrypted .
   iii. Optional storage scaling capabilities to accommodate future organizational needs.
   iv. Support for mailbox management and usage reporting.

4.3.2 Multi-Device Access & Synchronization

a) Support access via web, desktop and mobile devices.
b) Real-time synchronization of emails, contacts, calendars, and tasks across all devices.
c) Secure authentication leveraging modern protocols.
d) Ensure consistent user experience during remote and roaming access scenarios.

4.3.3 Collaboration & Productivity Features

a) Shared calendars, shared mailboxes or equivalent, resource scheduling, distribution lists, and groups.
b) Task management and internal chat/messaging functionality integrated or available via OEM suite.
c) Integration with Active Directory or equivalent Identity Management tool (IAM)
d) Address List/ Address Book Management

4.4 Email Security (For 1500 Users)

a) The Service Provider shall deploy an enterprise-grade, comprehensive email security layer protecting 1500 users against modern threats.

4.4.1 Advanced Threat Protection

a) Detection and prevention of spam, phishing, spoofing, ransomware, malware attacks, etc.

b) Zero-day threat protection via sandboxing, dynamic scanning, and behavioral analysis.

c) Time-of-click URL protection preventing access to malicious links.

d) Malicious attachment analysis with quarantine and remediation capabilities.

4.4.2 Secure Email Transmission & Storage

a) Enforce end-to-end encryption for message transport and data encryption

4.4.3 Identity & Access Controls

a) Implement role-based access control (RBAC) with granular permissions and audit logging.

b) Support multi-factor authentication (MFA) and password-less authentication methods.

c) Maintain detailed, tamper-proof audit trails for all administrative and user activities related to email access and configuration.

4.4.4 Compliance & Policy Enforcement

a) Enforce organizational policies on email signatures, disclaimers, and DLP in outgoing emails.

b) Generate periodic compliance and security posture reports aligned with CERT-In guidelines.

4.5 Data Protection Solution

4.5.1 Data Protection – Email (1500 Users)

a) Implement policy-driven Data Loss Prevention (DLP) to prevent unauthorized sharing, forwarding, or exporting of sensitive information.

b) Identification and protection of sensitive data such as Aadhaar numbers, PAN, Personally Identifiable Information (PII) using predefined templates.

c) Conditional access evaluation based on device and user context.

   i. Alert IT/security teams automatically upon DLP policy violations with actionable incident response workflows.

4.5.2 Data Protection – Endpoint (2000 Endpoints)

a) Implement policy-driven Data Loss Prevention (DLP) to prevent unauthorized sharing, forwarding, or exporting of sensitive information.

b) Maintain comprehensive logging of sensitive data usage and policy violations, with regulatory-compliant reporting dashboards.

c) Inline controls to block or restrict downloads, uploads, copy, print, and sharing operations by any medium based on policies.

4.6 Backup Solution

4.6.1 Backup – Email (1500 Users)

a) Set up automated, policy-driven, full and incremental backups with customizable retention schedules for all mailboxes, shared mailboxes, and groups.

b) Configurable retention policies tailored to business and regulatory needs.

c) Provide granular restore functionalities enabling recovery at the individual email, folder, or complete mailbox level.

- Individual emails
- Selected folders
- Complete mailboxes

d) Schedule and execute regular backup integrity checks and recovery drills to validate restoration capabilities.

e) Offer centralized monitoring dashboards showing backup status, alert on failures, and summarize compliance metrics.

4.6.2 Backup – Endpoint (2000 Endpoints with 20 TB capacity)

a) Backup solution supporting 2000 endpoints with a minimum aggregated storage pool of 20TB.

b) Automated continuous or scheduled backup of user files, folders, profiles, and system states.

c) Full system restores capabilities on supported endpoint platforms.

d) Support granular restore options covering single files, folder structures, user profiles, and full system restore on supported platforms.

e) Secure backup storage

f) Compliance and audit-ready reporting dashboards covering backup activities and retention metrics.

i. Provide real-time monitoring and reporting capabilities integrated into the centralized IT management console.

4.6.3 Backup Schedule and Frequency

a) Backup retention policies must ensure that backups are retained for a minimum duration as per applicable guidelines for each component and full backups for at least one year, in compliance with organizational and regulatory requirements.

b) Automated verification and validation of backup integrity shall be performed weekly to guarantee recoverability of data.

c) All backup data shall be securely stored within Indian Data Centers, featuring immutability capabilities to prevent unauthorized alteration or deletion.

d) Real-time monitoring and reporting of backup activities shall be integrated into the centralized IT management dashboard to provide operational visibility and compliance assurance.

4.6.4 Backup Schedules and Frequency:

Backup Type	Frequency	Time Window (Off-Peak)	Description	Retention Period	Additional Requirements
Continuous Backup	It will be finalized during Implementation Stage	It will be finalized during Implementation Stage	Automated backup of user files, folders, and profiles throughout business hours	N/A	Changes outside business hours backed up in next cycle
Full Backup	It will be finalized during Implementation Stage	It will be finalized during Implementation Stage	Complete backup of all endpoints and system states	Minimum 1 year	Ensure minimal operational impact during backup
Incremental/ Differential Backup	It will be finalized during Implementation Stage	It will be finalized during Implementation Stage	Captures changes since last full or incremental backup	Minimum 90 days	Scheduled to balance performance and data protection
System State Backup	It will be finalized during Implementation Stage	It will be finalized during Implementation Stage	Backup of system state for full system restore capability	Aligned with full backup retention	

Backup Type	Frequency	Time Window (Off-Peak)	Description	Retention Period	Additional Requirements
Backup Validation	It will be finalized during Implementation Stage	It will be finalized during Implementation Stage	Automated verification of backup integrity and recoverability	N/A	Document failed jobs and corrective actions; maintain reports for audit.
Backup Restore Testing	It will be finalized during Implementation Stage	It will be finalized during Implementation Stage	Tests restore of selected files, systems, and/or full environments to verify recoverability.	N/A	Maintain records of test results, issues found, and resolution.
Backup Storage Security	It will be finalized during Implementation Stage	It will be finalized during Implementation Stage	Secure storage within Indian Data Centers with immutability	As per retention policy	Integration with centralized monitoring and reporting

4.6.5 Restoration Policy

Backup Period	Restoration Frequency
Backup taken in last month	It will be finalized during Implementation Stage
Backup taken in last quarter	It will be finalized during Implementation Stage

4.7 General Requirements for All Solution Components

a) End-to-end encryption for data at rest and in transit.

b) Centralized monitoring, including dashboards and real-time incident alerting.

c) Integration with Active Directory for user identity lifecycle and access management.

d) Ensure compliance with Government of India cybersecurity directives and applicable data protection regulations.

e) 24×7 remote monitoring, support, and incident response capability.

f) Comprehensive documentation for deployments and configurations.

g) Training and handover sessions for administrators and end-users ensuring smooth adoption.

h) Support for periodic updates, patching, upgrades, and continuous improvement.

i) The Bidder shall submit a proposal setting forth a solution that is in strict and complete conformity with the Technical Requirements specified in Annexure X, and shall not introduce or rely upon any deviation, exception, or non-compliance thereto.

4.8 Support and Training

a) OEM shall provide **24×7 remote monitoring and support** for all deployed solutions, including email, security, data protection, and backup components.

b) The Selected Service Provider/Vendor shall provide round-the-clock (24×7) remote monitoring, incident management and support services for the Services, in accordance with the Service Levels (SLAs) specified in this Agreement and/or the Service Level Agreement annexed hereto.

c) The Service Provider/Vendor shall furnish system-generated reports evidencing such monitoring, incidents, resolution activities and SLA compliance on a quarterly basis, and shall submit the said reports along with the corresponding quarterly invoices for the Services. Failure to submit such reports may be treated as non-compliance with the terms of this Agreement, without prejudice to the Purchaser's/Client's other rights and remedies hereunder.

d) Rapid incident detection, acknowledgement, escalation, and resolution to ensure minimal downtime and impact.

e) Proactive health monitoring, alerting, and regular patching, updates, and upgrades of all solution components.

f) A help desk shall be available for user support via email, phone, and chat.

g) Comprehensive training shall be provided for administrators covering deployment, configuration, monitoring, troubleshooting, and reporting.

h) Provide detailed documentation, user manuals, quick reference guides, and video tutorials.

4.9 Ongoing Maintenance and Configuration

a) The bidder shall configure and update features as per technical compliance and evolving MIDC requirements throughout the contract period.

b) Backup and Data Loss Prevention (DLP) policies shall be configured and updated as required by MIDC during the contract period.

c) The bidder will assist MIDC in leveraging all features and functionalities available in their subscribed email solution plans and related components.

d) The bidder shall maintain detailed records of any downtime, facilitating the claims procedure and adherence to service credit policies.

e) Disclosure of any data related to the email solution shall be strictly regulated and shared only upon explicit approval from MIDC.

f) The bidder and OEM shall provide MIDC full access to all security logs related to email environments, critical for incident analysis and response improvements.

g) The bidder is responsible for ensuring data confidentiality, privacy, and system access controls for the entire deployed solution.

h) All software upgrades provided by the OEM will be deployed by the bidder for free whenever requested by MIDC.

i) The bidder shall deploy all latest updates and infrastructure upgrades within three months of their release.

j) All product updates, upgrades, and patches shall be provided free of cost during the entire contract period.

k) The bidder shall ensure that all software solutions are legally licensed; detailed license counts and license types must be clearly provided.

l) Upon request, the bidder and OEM shall furnish all relevant data, audit reports, and records to MIDC-appointed auditors, inspecting officials, or regulatory authorities.

m) Any deficiencies found during audits or reviews must be promptly addressed and resolved by the bidder and OEM, with documented evidence of remediation and certification provided to MIDC.

4.10 Data Ownership

a) MIDC shall retain sole ownership and rights over all data stored on its tenant. Data shall never be considered the service provider's asset and the bidder shall take all necessary measures to protect data security and privacy. The bidder must promptly notify MIDC of any data breaches or legal processes affecting MIDC data and support MIDC with data removal requests, providing confirmation of deletion. The bidder shall ensure timely backup and recovery arrangements that meet MIDC's satisfaction.

b) Policies shall be aligned with MIDC's existing security frameworks and as per industry best practices.

c) Regular monitoring, reporting on email security threats, and compliance with MIDC's data protection policies and regulatory requirements are mandatory.

d) MIDC's password management and session timeout policies shall be replicated accurately within the Cloud Email tenant.

e) Mailbox audit logging shall be enabled to ensure compliance and traceability of email activities.

f) The bidder shall provide documented Standard Operating Procedures (SOPs) covering all technical configurations, known issues, and process changes.

g) A comprehensive endpoint backup solution with up to 20 TB capacity shall be provided, including scheduling, monitoring, testing, and recovery procedures to assure business continuity.

h) SOPs for backup operations, recovery testing, and incident handling related to endpoint data backup shall be developed and shared with MIDC.

i) Backup and recovery processes for 1500 email mailboxes, including shared mailboxes and groups, shall be maintained according to MIDC's retention policies.

j) Procedures enabling fast restoration of email data in cases of data loss or corruption shall be documented and tested to ensure data integrity and availability.

4.11 Migration and Integration

a) The Bidder shall be solely responsible for the complete migration of the existing e-mail services to the proposed e-mail services, as well as the migration of all associated drive data, in a seamless manner and without any loss, alteration, or corruption of e-mails or data.

b) The Bidder shall ensure that all existing mailboxes, e-mails, folders, attachments, configurations, and drive data are fully and accurately migrated and made available in the new environment. Any loss or corruption of e-mails or data arising out of or in connection with the migration shall be remedied by the Bidder at its own cost, without prejudice to the Purchaser's/Client's other rights and remedies under the Contract.

c) In case any third-party software required for migration, bidder will bear cost of the same

d) Bidder must submit migration plan and timelines along with RFP

A) Data Migration Strategy

a) Conduct a thorough assessment of existing email systems and interfaces with business-critical applications.

b) Develop comprehensive migration plans ensuring zero mail flow disruption during the migration of primary and archive mailboxes, including encrypted messages.

c) Provide proprietary or third-party migration tooling for efficient migration of mailbox data.

B) Migration Phase:

a) All the primary, individual as well as common, mailboxes hosted on the existing mail server shall be migrated.

b) Migration of mailboxes shall be done into i.e. all the mails, calendars, contacts, folders, subfolders contained within a mailbox including encrypted mails as at the time of migration should be migrated irrespective of number/ age of mails, size of mailbox etc.

c) Migration of archive mailboxes of individual users

d) Any additional software tool required for the migration of mailboxes shall be the responsibility of the bidder and MIDC will not make any additional payments towards the same.

e) Service Provider shall ensure that during migration activity, there is no mail communication disruption faced by MIDC as well as external users.

f) The bidder must configure security policies in accordance with the existing IT security posture.

C) Existing Domain Compatibility and Integration:

a) The bidder is expected to ensure a seamless transition by integrating with existing infrastructure, maintaining user experience, and providing necessary tools for AD and domain mapping.

b) Domain Name and DNS Integration

i. **Mail Flow Continuity:** The bidder must ensure continuous email flow during the migration, including DNS record updates for the existing domains.

ii. **Support for Existing and New Domains**: The solution must support the existing domain names, enabling users to continue sending and receiving emails using their current email addresses without disruption. In the event a new domain name is procured, the Bidder shall also provide all necessary configuration, migration, and support services to align the new domain with the existing domain environment, including coexistence, redirection/forwarding, and preservation of user access, without impacting ongoing email services.

4.12 Tentative Roles and Responsibilities in Consortium

a) Bidder and Consortium Member should define their respective scope in Consortium Agreement and submit with the technical proposal

b) The typical partners in the consortium may include the following:

c) Primary Partner (Lead Bidder): (only 1)

i. The Lead Bidder shall act as the **Single Point of Contact (SPOC)** for MIDC and shall hold the ultimate contractual and financial responsibility, ensuring that all consortium members meet their

respective obligations. The Lead Bidder shall act as the **System Integrator (SI)** and shall be responsible for the supply, installation, and commissioning of the proposed solution

d) Consortium Members: (up to 1 members)

i. Email Security/Data Protection/Backup solution Partner: Focuses on implementing tools like DLP and Backup

5. Estimated Project Timelines, Payment Terms and Deliverables

Sr. No.	Description	Project Timelines	Payment Terms	Document Required
1	**Issuance of Work Order**	Start Date = 'T'		PBG to be submitted within 15 days from the issuance of Work Order
2	**Pre – Implementation:** Project Plan and Solution Design	'T' + 15 days		Submit Project Plan and Solution Documents with acknowledgment from IT Department
3	**Migration of Email Services**	'T' + 30 Days	100% after migration	Delivery and Installation report for respective location from IT Dept / MIDC concerned person for respective location
4	**Implementation:** Supply & Activation of Subscription / Licenses for Product & Services (other than email)	'T' + 30 days	40% of rate quoted under the line item "A. Licence subscription cost Line item 5 to 9"	Subscription activation report / Software License with acknowledgment from IT Department
5	**Implementation:** Installation, Configuration and Testing of proposed product and services (other than email)	'T' + 60 days	60% of rate quoted under the line item "A. Licence subscription cost Line item 5 to 9"	Installation report with acknowledgment from IT Department
6	**Email Subscription Charges**	Yearly	No of Users will be calculated on Monthly Basis. Min quantity will be 1000 users/mailboxes communicated by MIDC	Submit Quarterly Invoice
7	**Operation & Maintenance**	2 years	Payment will be made per locations as per rate quoted under line item "Operation & Maintenance"	Submit Quarterly Invoice

Sr No	Phase	Deliverables	Timeline
1	Pre-Implementation	• Solution design document for email solution • Architecture design, Project plan and timeline • Compliance and security assessment • Email security policy and architecture document • Security solution design and integration plan • Endpoint inventory and classification report • Backup strategy and policy document • Backup architecture design • Storage and retention plan • Compliance and recovery point objective (RPO) definitions	To be submitted along with Technical Bid
2	Migration of Email	• Report on the successful migration of all the existing emails • Report on the migration of data from existing email solutions. • Report on the successful migration of archival data. • Report on the migration certifying zero data loss of existing emails.	To be completed within 30 days from Issuance of Work Order
3	Implementation of other product / services	• Activation of email security services • Enablement of data protection features (email & endpoints) • Endpoint agent roll-out completion report • Data protection policy enforcement logs • Full implementation of backup solutions • Backup schedules activated • Backup monitoring and reporting system setup	To be completed within 60 days from Issuance of Work Order
4	Post-Implementation	• System stability and usage reports • SLA adherence report • User feedback and issue resolution logs • Final project closure report • Security incident and resolution reports • Continuous monitoring and alert summaries • Regular update and patch management logs • Periodic data protection audit reports • Endpoint compliance and security posture reports • Data loss prevention incident analysis • Backup health and restore success reports • Periodic backup audit and compliance reports • Disaster recovery test reports	On Quarterly Basis

6. Service Level Agreement (SLA)

6.1 Purpose

The purpose of this Service Level Agreement (SLA) is to clearly define the levels of service that the selected Agency (Service Provider) shall provide to MIDC for the duration of the Cloud-based Email Solution contract. This SLA stipulates the minimum expected service quality, performance metrics, and the accountability framework to ensure reliable, secure, and timely email communication services, as well as robust email security, data protection for email and endpoints, and backup services for both endpoints and email systems.

6.2 General SLA Framework

a) The SLA timelines correspond to the Payment Terms detailed in Section 7 and constitute minimum delivery requirements**.**

b) The Service Provider shall continuously monitor all services—including Email Security, Data Protection (Email and Endpoint), Backup (Endpoint and Email), and Cloud-based Email Services—and ensure compliance with performance levels.

c) Quarterly reviews shall be conducted by MIDC to:

   i. Evaluate service performance against SLAs, track incident trends, and review major issues across all service domains including security, data protection, and backup.

   ii. Discuss escalated problems, unresolved matters, and corrective action status.

   iii. Incorporate any MIDC-driven suggestions for service enhancement.

d) MIDC reserves the right to initiate interim reviews or independent audits of the tools, techniques, and procedures adopted by the Service Provider while safeguarding security and confidentiality.

e) Performance review meetings will be scheduled mutually with representatives from both MIDC and the Service Provider expected to attend.

f) SLA metrics incorporate:

   i. Equipment/Infrastructure Availability (including Email Security, Data Protection, and Backup systems)
   ii. Technical Helpdesk Support Services
   iii. Compliance and Reporting Procedures for email, security, data protection, and backup services

6.3 SLA Applicability & Scope

a) The SLA is an integral contractual component ensuring the Service Provider’s accountability for uptime, quality, and timeliness for Cloud based email, Email Security, Data Protection (Email and Endpoint), and Backup (Endpoint and Email).

b) Uptime computation excludes:

   i. Downtime caused by failures of MIDC's IT infrastructure or third-party components not controlled by the Service Provider.

c) Issues arising from MIDC's negligence or failures in applications/services provided by MIDC or its vendors.

d) The Service Provider bears the responsibility to prove outages attributed to MIDC or external factors beyond their control.

6.4 Defined SLAs

6.4.1) Implementation & Migration

Parameter	Target	Penalty
Migration of 1500 users from existing email services to the newly proposed email solution, includes Email Security for 1500 users, Data Protection for Email for 1500 users, Data Protection for Endpoint for 2000 devices, Backup for Endpoint (20 TB) for 2000 devices, Backup for Email for 1500 users	To be completed within 30 days post-migration from the existing email solution.	0.25% of total order value per day of delay

6.4.2) Cloud-based Email Services

Parameter	SLA Target	Penalty on Quarterly Payment
Email Service Uptime	≥ 99.9%	No penalty
Email Service Uptime	< 99.9% and ≥ 99.0%	10% Penalty
Email Service Uptime	< 99.0% and ≥ 95.0%	15% Penalty
Email Service Uptime	< 95.0%	20% Penalty

*Note: Uptime calculated quarterly as:

$$\text{Uptime \%} = \left(\frac{\text{Total Minutes in Quarter} - \text{Downtime Minutes}}{\text{Total Minutes in Quarter}}\right) \times 100$$

6.4.3) SMTP Server, Active Directory Services, Data Protection, and Backup Services

Parameter	SLA Target	Penalty per Occurrence
Uptime	≥ 99.9%	No Penalty

Parameter	SLA Target	Penalty per Occurrence
Uptime	≥ 98.0% and < 99.9%	10% Penalty
Uptime	≥ 95.0% and < 98.0%	15% Penalty
Uptime	< 95.0%	20% Penalty

- Downtime must not exceed consecutive 10 minutes to avoid breach.

Note: Uptime calculated quarterly based on total downtime in the quarter.

6.4.4) Helpdesk and Issue Resolution

Severity Level, Response Time, Resolution Time, and Penalties apply to issues across Email Services, Email Security, Data Protection, and Backup Services as follows:

Severity Level	Response Time	Resolution Time	Penalty (per Incident)
Critical (Severity 1)	≤ 30 minutes	≤ 1 day	Rs. 10,000 per hour/day delay in response or resolution
Medium (Severity 2)	≤ 1 hour	≤ 2 days	Rs. 7,500 per day delay
Low (Severity 3)	≤ 2 hours	≤ 4 days	Rs. 5,000 per day delay

- Average Ticket Lost Rate: % monthly;
  Penalties Rs. 1,000 for each additional 1% lost tickets per quarter (tickets that were unattended / unresolved).

6.4.5) Security Breaches

Parameter	Target	Penalty
Data and Security Breaches across Email, Endpoint Data Protection, Backup, and Security	Zero Breaches	Rs. 1,00,000 per breach/incident

- Covers any breach or compromise of MIDC's data or security attributed to the Service Provider.

6.4.6) Reporting

Report Type	Delivery Timeline	Penalty
Quarterly Reports & Dashboards	By 15th of every quarter for previous quarter	Rs. 10,000 per day delay
Implementation Phase Reports	Within 15 days post completion	Rs. 10,000 per additional week delay

- Report format to be mutually finalized at project inception**.**

6.4.7) Consolidated SLA Table

Sr No	SLA	Parameter	Measurement	Target / Threshold	Penalty
A. Milestone - Phase - 1 (Implementation)					
1	**Implementation & Migration**	Full scope migration (Email 1500 users; Email Security 1500; Data Protection for Email 1500; Endpoint Data Protection 2000 devices; Endpoint Backup 20 TB for 2000 devices; Email Backup 1500 users)	T = Purchase Order date	To be completed within 30 days post migration from existing email solution	**0.25% of total order value per day of delay**
B. Quarterly Operations - Phase – 2 (Operations)					
2	**Cloud-based Email Services**	Email Service Uptime	Uptime calculated quarterly: Uptime % = ((Total Minutes in Quarter − Downtime Minutes) / Total Minutes in Quarter) × 100 Quarterly measurement	≥ 99.9%	No penalty
				< 99.9% and ≥ 99.0%	**10% penalty** on quarterly payment
				< 99.0% and ≥ 95.0%	**15% penalty** on quarterly payment
				< 95.0%	**20% penalty**
3	**SMTP Server, AD Services, Data Protection, Backup**	Uptime	Uptime calculated quarterly based on total downtime	≥ 99.9%	No penalty
				≥ 98.0% and < 99.9%	**10% penalty per occurrence**
				≥ 95.0% and < 98.0%	**15% penalty per occurrence**
				< 95.0%	**20% penalty per occurrence**
		Downtime breach condition	Applies per occurrence	Consecutive downtime must not	Breach if exceeded

Sr No	SLA	Parameter	Measurement	Target / Threshold	Penalty
				exceed **10 minutes**	
4	**Helpdesk & Issue Resolution**	Severity 1 (Critical) – Response Time	Resolution time **as mutually agreed with MIDC**	≤ 30 minutes	**₹10,000 per hour/day delay** in response or resolution
		Severity 1 (Critical) – Resolution Time	Applies per incident	As mutually agreed	**₹10,000 per hour/day delay**
		Severity 2 (Medium) – Response Time		≤ 1 hour	Included in penalty model below
		Severity 2 (Medium) – Resolution Time	Per incident	≤ 2 days	**₹7,500 per day delay**
		Severity 3 (Low) – Response Time		≤ 2 hours	Included in penalty model below
		Severity 3 (Low) – Resolution Time	Per incident	≤ 4 days	**₹5,000 per day delay**
		Average Ticket Lost Rate	Lost = unattended/unresolved	≤ 1% monthly	**₹10,000 per additional 1% lost tickets per quarter**
5	**Security Breaches**	Data/Security Breaches (Email, Endpoint, Backup, Security)	Any breach or compromise attributed to Service Provider	**Zero breaches**	**₹1,00,000 per breach/incident**
6	**Reporting**	Quarterly Reports & Dashboards	Format mutually finalized at project inception	By **15th** of every quarter (for previous quarter)	**₹10,000 per day delay**
		Implementation Phase Reports		Within **15 days** post completion	**₹10,000 per additional week delay**

Note:

- Penalty for Phase 1 - Implementation 1 is capped at a maximum of 10% of Total Contract Value .
- Penalty for Phase – 2 (Operations) **is** capped at a maximum of 20% of the quarterly payment.

6.5 Performance Review and Audits

a) MIDC will hold quarterly performance review meetings with the Service Provider to assess all service areas including Email Security, Data Protection (Email and Endpoint), Backup (Endpoint and Email), and Cloud-based Email Services.

b) MIDC reserves the right to conduct surprise audits and inspections of tools, processes, and security compliance—including Email Security controls, Data Protection mechanisms, and Backup integrity—by engaging third-party experts without compromising confidentiality or security.

6.6 Incident Classification and SLA Response Times

Incident Category	Definition/Description	Time Target	Resolution Time Target
Critical	Incidents causing complete loss of service or major degradation severely impacting business operations. Includes total link outage or security breach.	Response within 30 minutes	Resolution within 2 hours
High	Incidents causing significant degradation, but partial service is available. Operations are impacted but workarounds may be available.	Response within 1 hour	Resolution within 4 hours
Medium	Incidents causing minor degradation or impacting non-critical services, with minimal effect on business operations.	Response within 4 hours	Resolution within 8 hours
Low	Incidents with no immediate impact on service or business operations, such as informational requests or minor issues.	Response within 8 hours	Resolution within 24 hours

6.7 Review & Governance

a) **Quarterly SLA Review Meetings** with MIDC IT and Operations teams

b) **Continuous Improvement Plans** based on performance trends

c) Escalation Matrix to be maintained and updated by the Selected Agency

7. Payment Terms and Schedule

7.1 Payment Terms

a) This Project is planned to be implemented as a service complete with all the components and solution required for delivery of the envisaged activities of the Project. The bidder will be compensated for such Services, subject to the performance of the system as reflected by the SLA metrics defined in the Agreement and/or the MSA between the Bidder and Department.

b) The entire cost for establishing, operating and maintaining the Project for the Contract Period will be borne by the Bidder and factored in his Commercial Proposal submitted in response to the RFP.

c) The Costs quoted will be considered for the computation of Total Contract Value (TCV).

TCV = Finalized amount agreed upon between dept against amount quoted by bidder in Annexure XI.

d) The Total Amount against Total Contract Value quoted in the Commercial Proposal should cover all costs anticipated by the Bidder, on the basis of requirements listed in the RFP. This would include, but not be limited to:

e) Cost of Inventory and Licenses

f) Cost of Installation and commissioning as mentioned in RFP.

g) Operations and comprehensive maintenance costs for 2 years after 'Go-live'.

h) Any other anticipated costs for providing the Services mentioned the RFP and for achievement of SLAs.

i) The Bidder will be solely responsible to bear the cost of any items that are not quoted or are under quoted in this Proposal but are required to meet the SLAs or any other requirements as stated in the RFP. No additional payment for these components would be made to the Bidder.

j) The payment towards Milestone Implementation to be paid on actuals after the successful procurement and deployment of the licenses and tools on the infrastructure. MIDC may carry out the online verification before making the payment.

k) Except as otherwise provided for herein or as agreed between the parties in writing, the Department shall not be required to make any payments in respect of the Services other than those covered by this RFP.

l) The Bidder would be paid as per the details given in the Payment Milestones and Schedules.

m) If, and only if, MIDC intends to procure additional licenses over and above the quantities specified in the RFP, the bidder shall supply such additional licenses at the rates quoted in the commercial proposal

7.2 Invoicing and Settlement

a) The Bidder will submit its invoices in accordance with the following principles.

b) Generally, and unless otherwise agreed in writing between the parties or expressly set out in the Master Services Agreement or the SLA, the Bidder shall raise an invoice for successful completion of an operational quarter after Go-live as per the Payment Schedule defined in Section 5. of this RFP.
c) The invoice shall be submitted along with the necessary approval / signoff / acceptance / certification provided by the concerned parties for the respective Deliverables linked with the milestone or Quarter, failing which the Department reserves the right to reject the invoices.
d) Along with the invoice, the Bidder is required to submit the Deliverables linked with the payment in softcopy and hardcopy formats, as applicable failing which Department reserves the right to reject the invoices.
e) Any invoice presented in accordance with this Schedule shall be in a form agreed with the Department.
f) Invoices shall be accurate and all adjustments (if any) to payments to be made to the Bidder shall be applied to the next payment invoice of the Bidder.
g) For Quarterly invoices, payment of the invoice amount will be made within 90 days of the receipt of correct and valid invoice by the Department. The invoice amount will be released by the Department within 90 days of the receipt of the invoice on completion of detailed bill vetting.
h) Payment for invoices, which has to be upon completion of the said activities, and after obtaining the signoff from the Department for the required Deliverables and is subject to penalties / adjustments based on the SI's performance.
i) The penalties are imposed on the Bidder as per the SLA criteria specified in Section 6 of this RFP.
j) The Milestone invoices related amount will be released by the Department within 90 days of the receipt of the invoice on completion of detailed bill vetting and penalty calculations as per the defined SLAs.
k) The Department shall be entitled to delay or withhold payment of any invoice or part of it delivered by the Bidder where:
l) The Department disputes such invoice or part of it provided that such dispute is bona fide.
m) The Department disputes any previous invoice or part of it that it had not previously disputed under this RFP provided that such dispute is bona fide.
n) The withheld amount in both the above cases shall be limited to that which is in dispute. The disputed amount in both the above cases shall be referred to the procedure as set out in Section 3.28. Any exercise by the Department under this Section shall not entitle the Bidder to delay or withhold provision of the services.

7.3 Additional Costs

a) The Department shall make payments to the Bidder at the times and in the manner set out in the Terms of Payment Schedule subject always to the fulfilment by the Bidder of the obligations herein.
b) All payments shall be made after adjustments required for any SLA based penalties.

c) No invoice for extra work / change order on account of change order will be submitted by the Bidder unless the said extra work / change order has been authorized / approved by the Department in writing in accordance with Additional works framework of the RFP.
d) The Department shall make payments after withholding tax deductible at source as mentioned above.
e) The prices should be mentioned without any qualifications whatsoever and should include all taxes, duties, fees, levies and other charges as may be applicable in relation to the activities proposed to be carried out. It is mandatory that such charges wherever applicable/ payable should be indicated separately. For the project bid, the Bidder is expected to take into account all taxes except GST.

7.4 Currency of Payment

a) Payment shall be made in Indian Rupees only.

7.5 Taxes and Statutory Payments

a) The Bidder shall bear all personal / income taxes levied or imposed on its staff, vendor etc. on account of payment received under the contract. The Bidder shall bear all income/corporate taxes, levied or imposed on the Bidder on account of payments received by it from the Department for the work done under the contract.
b) The Department or its nominated agencies shall be responsible for withholding taxes from the amounts due and payable to the Bidder wherever applicable. The Bidder shall pay for all other taxes, duties or levies in connection with the MSA, SLAs, and any other Project Engagement Definition including, but not limited to, goods and services and other applicable taxes, duties or levies.
c) The Department or its nominated agencies shall provide the Bidder with the original tax certificate of any withholding taxes paid by the Department or its nominated agencies on payments as per the MSA. The Bidder agrees to reimburse and hold the Department or any of its nominated agencies harmless from any deficiency (including penalties and interest) relating to taxes that are its responsibility under this paragraph. For purposes of MSA, taxes, duties or levies shall include taxes, duties or levies incurred on transactions between and among the Department, the Bidder.
d) In the event of any increase or decrease in the rate of GST, the consequential effect shall be to the accounts of the Department.
e) In the event of any increase or decrease of any other tax, levies, currency exchange rates etc. due to any statutory notification(s) during the term of the MSA, the consequential effect shall be to the account of the Bidder.
f) The parties shall cooperate to enable each party to accurately determine its own tax liability and to minimize such liability to the extent legally permissible. In connection therewith, the parties shall provide each other with
    i. Any resale certificates,
    ii. Any relevant information regarding use of out-of-state materials, equipment or services and

iii. Any exemption certificates or information reasonably requested by the other party.

7.6 Liquidated Damages

a) In addition to the penalty as mentioned in the SLA, liquidated Damages will be levied on the SI, in the event of the SI:
   i. Failing to meet the milestones provided for in the MSA,
   ii. Failing to perform the responsibilities and obligations as set out in MSA.

b) Department shall be entitled without prejudice to its other rights and remedies, to deduct from the price payable to the Bidder and also to encash the Performance Bank Guarantee, provided the total amount recovered does not exceed 25% of Total Contract Value or the insurance cover, whichever is higher.

8. Evaluation Process

A) Opening of Bids

a) The bids that are submitted online successfully shall be opened online as per date and time given in Proposal Data Sheet, through MahaTender procedure on the scheduled date.

b) Bids shall be opened either in the presence of bidders or it's duly authorized representatives, if the bidders choose to attend the same. The bidder representatives who are present shall sign a register evidencing their attendance. Two representatives per applicant shall be permitted to be present at the time of opening the tender. In addition to that, if their representative of the Bidder remains absent, MIDC will continue process and open the bids of all Bidders.

c) Total transparency will be observed and ensured while opening the Proposals/Bids.

d) MIDC always reserves the rights to postpone or cancel a scheduled Bid opening.

e) Bid opening will be conducted in two stages

   i. In the first stage, Pre-qualification Proposals and Technical proposals would be opened. The EMD payment and tender fee payment will be verified from the MahaTender Portal. Pre-Qualification and Technical Evaluation will be carried out by the Bid Evaluation Committee (BEC) constituted by MIDC. Authority may choose to seek the clarifications on the pre-qualification and technical bids during the evaluation stage.

   ii. In the second stage, Commercial Proposal of those Bidders whose Pre-qualification and Technical Proposals qualify, would be opened.

   iii. In the event of the specified date of Bid opening being declared a holiday for MIDC the bids shall be opened at the same time and location on the next working day.

9. Pre-Qualification (PQ) Criteria

All the bidding entities should fulfil the PQ criteria mentioned below. Only entities fulfilling these criteria, will be considered for the Technical and Financial evaluation of the bid.

PQ	Bidder's Eligibility Criteria	Descriptions	Remarks Documents Required
1	Tender Fees	The sole bidder or consortium member should have made a payment of Rs. 1,20,000 (Rupees One Lakh Twenty Thousand only) for the tender fees.	Proof of Tender form fee payment of Rs. 1,20,000/- (Rupees One Lakh Twenty Thousand only) (non-refundable) through online payment gateway available at the e-tendering portal
2	Earnest Money Deposit (EMD)	The sole bidder or consortium member should have submitted an Earnest Money Deposit (EMD) of Rs. 12,00,000/- (Rupees Twelve Lakhs only)	EMD payment receipt generated from the e-tendering portal. EMD to be paid through online payment gateway available at the e-tendering portal
3	Tender Fees and EMD for MSMEs	Tender fees and Earnest Money Deposit are to be obtained from the bidders except Micro and Small Enterprises (MSEs) as defined in MSE Procurement Policy issued by Department	Valid Certificate issued to the bidder to be produced that they are registered either with Department of Micro, Small and Medium Enterprises (MSME) or are registered with the Central Purchase Organisation or the concerned Ministry or Department.
4	Local Presence	The sole bidder and consortium member should have their offices/ branch offices in Maharashtra.	Proof of Address (Self Attested copy of Telephone bill / Electricity Bill / Property tax bill / Registered Rent Deed supporting the address at Maharashtra) in addition to the documents asked above
5	Legal Entity	The sole bidder and consortium member should be: • A company incorporated in India under the Companies Act, 1956 / 2013, and subsequent amendments thereto. • Registered with GST Authorities in India • Operating for the last five years in India as on the date of publishing of RFP notice (including name	a) Certificate of Incorporation & Memorandum and Articles of Association of Bidder to be enclosed along with full address of Registered office. OR b) A partnership deed duly registered under the Partnership Act OR c) LLP firm registered certificate.

PQ	Bidder's Eligibility Criteria	Descriptions	Remarks Documents Required
		change / impact of mergers or acquisitions). *Note: In case of consortium, maximum 1 consortium members are allowed.	AND d) Copy of PAN Card
6	Financial Strength – Turnover	Minimum Average Annual Turnover of Bidder should be at least Rs. 60 Crore or more in last 3 years as mentioned i.e., (FY 2022-2023, 2023-2024 and 2024-25) to qualify Minimum Average Annual Turnover of Consortium should be at least Rs. 4 Crore in last 3 years as mentioned i.e., (FY 2022-2023, 2023-2024 and 2024-25) to qualify	Audited Balance sheet and Profit & Loss account statement of the Bidder for any of the last 3 audited financial years (FY 2022-2023, 2023-2024 and 2024-25) & Certificate duly signed by Statutory Auditor of the Bidder or Certified Chartered Accountant for average annual Turnover for last 3 financial years (FY 2022-2023, 2023-2024 and 2024-25) (As per Annexure-III)
7	Financial Strength – Net-worth	The sole bidder or lead bidder and Consortium bidder should have a *positive net worth* in last three financial years (FY 2022-2023, 2023-2024 and 2024-25).	Financial Audited balance sheets & Profit /loss statement, Statutory Auditor's Report, Notes to Accounts and Schedules forming part of accounts to be submitted. & Certificate duly signed by Statutory Auditor of the Bidder or Certified Chartered Accountant. As per Annexure-III
8	Similar Projects Experience (Email Solution)	The Lead / Sole Bidder should have experience of supply / implementation of at least one (1) project of Email solution in State / Central Government or Public Sector Unit (PSU) in last five years as on bid submission date	Client Certificate, Copy of Work Order/ Agreement & Annexure VIII
9	Similar Projects Experience	The Lead / Sole Bidder or Consortium bidder should have experience of supply / implementation of at least one	Client Certificate, Copy of Work Order/ Agreement

PQ	Bidder's Eligibility Criteria	Descriptions	Remarks Documents Required
	(Data Leak Prevention (DLP / Backup Solution)	(1) project of Data Leak Prevention (DLP) / Backup Solution (Server/Endpoint) in State / Central Government or Public Sector Unit (PSU)	& Annexure VIII
10	Similar Projects Experience (Value)	The Lead / Sole bidder or consortium member should have experience of supply / implementation of cloud security / email service & security/ Data Leak Prevention (DLP) / Backup Solution for below project value in State / Central Government or Public Sector Unit (PSU) as on the date of bid submission 1 Project – 9 Crores or 2 Projects – 6 Crores or 3 Project of – 4 Crores Note: The Bidder shall clearly specify the project cost/amount for each of the following service components separately: (i) Cloud Security, (ii) E-mail Service and Security, (iii) Data Leak Prevention (DLP), and (iv) Backup Solution.	Client Certificate, Copy of Work Order/ Agreement & Annexure VIII
11	Proposed OEM Experience Cloud SSE (Secure Service Edge)	OEM should have experience of supply and deployment of cloud-based SSE solution of minimum 20000 users in single order for Government / Public Sector Unit (PSU) in India in last 3 years.	Self-Declaration on OEMs letter head confirming no. of users in Government / PSU (Single order) in India. Or Client Certificate, Copy of Work Order/ Agreement
12	OEM Authorization MAF	The sole bidder or consortium member should provide the MAF for all the proposed solution	Refer Annexure XIV. MAF from the OEM

PQ	Bidder's Eligibility Criteria	Descriptions	Remarks Documents Required
13	Power Of Attorney	The sole bidder must submit the power of attorney to specify an individual who will be authorized for legal and financial matters	Power of Attorney by the Company for its authorized representative on the Company Letterhead (Refer Annexure IV)
14	GST	The sole bidder and consortium member should have Goods Service Tax number Registration, as applicable and other such necessary trade / business registrations	Copy of GST Registration Certificate
15	OEM/Cloud Email service providers Qualifications Certifications	The sole bidder or consortium member should have any two certificates as below: 1. CMMI Process Level 3 or above. 2. ISO 9001:2015. 3. ISO 27001:2013 for Information Security Management System. 4. ISO/IEC 20000-1:2018.	Copies of the valid certificates from authorized agencies Online Link to verify the certificate from the website of issuing authority / partner or any other website (as applicable). URL of the website to be provided.
16	Non-Blacklisting	The sole bidder and consortium member should not be declared blacklisted or ineligible by any Central or State Government / Urban Local Bodies / Government Departments / Companies (Public / Private Sector) in India due to unsatisfactory past performance, corrupt, fraudulent or any other unethical business practices in last 5 yrs. as on date of bid submission.	Self-declaration by the bidder and consortium member on company letterhead duly signed by authorized signatory. (Refer Annexure V)
17	Non-withdrawal	The sole bidder and consortium member should not have withdrawn from similar government projects and should not have any contract termination from similar project with Central or State Government / Urban Local Bodies / Government Departments / Companies (Public / Private Sector) in India	Self-declaration by the bidder and consortium member on company letterhead duly signed by authorized signatory. (As per Annexure-VI)

PQ	Bidder's Eligibility Criteria	Descriptions	Remarks Documents Required
18	Data Security Declaration	The sole bidder and consortium member should submit a declaration as per Annexure XV.	Self-declaration by the bidder and consortium member on company letterhead duly signed by authorized signatory. (As per Annexure-XV)

10. Technical Qualifications

a) The evaluation of the technical bids will be done by Bid Evaluation Committee (BEC). Technical evaluation conducted by the BEC shall be final and binding on all the Bidders. Each Technical Proposal shall be assigned a technical score out of a maximum of 100 points.

b) Bidders who have qualified as per the Pre-Qualification Criteria of this RFP document shall be evaluated and scored by the Bid Evaluation Committee (BEC) based on a weighted point system assessing each Bidder's ability to satisfy the requirements set forth in the RFP Document.

c) Technical Evaluation of the bids would be carried as follows:

Sr. No.	Technical Parameters	Descriptions	Supporting Documents	Max. Marks
1	Annual Turnover	Minimum Average Annual Turnover of the sole bidder or consortium member in last 3 years • More than INR 120 crore - 20 Marks • More than INR 90 crore but ≤ INR 120 crore – 15 Marks • More than INR 60 crore but <= INR 90 crore – 10 Marks	Certification / Undertaking Letter	20
2	Project Experience (Email Solution)	Lead / Sole Bidder should have experience of supply / implementation of at least one (1) project of Email solution in State / Central Government or Public Sector Unit (PSU) in last five years as on bid submission date 1 Project – 5 marks 2-3 Projects – 7 Marks 4 Projects or more – 10 Marks	List of customers in Central / State / Corporation / PSU or Copy of Work Order / Agreement Letter & Client Certificate	10

Sr. No.	Technical Parameters	Descriptions	Supporting Documents	Max. Marks
3	Project Experience (Data Leak Prevention (DLP)/ Backup Solution)	Sole Bidder or Consortium bidder should have experience of supply / implementation of at least one (1) project of Data Leak Prevention (DLP) / Backup Solution (Endpoint / Server) in State / Central Government or Public Sector Unit (PSU) 1 Project of the same proposed DLP / Backup Solution – 10 Marks Or 1 Project of Any DLP / Backup Solution – 5 Marks	Work Order / Agreement Letter & Client Certificate	10
4	Similar Projects Experience (Value)	The Lead / Sole bidder or consortium member should have experience of supply / implementation of cloud security / email service & security/ Data Leak Prevention (DLP) / Backup Solution for below project value in State / Central Government or Public Sector Unit (PSU) as on the date of bid submission **10 Marks if bidder submits:** 1 Project of value 9 Crores or 2 Projects of value 6 Crores or 3 Projects of value 4 Crores Note: The Bidder shall clearly specify the project cost/amount for each of the following service components separately: (i) Cloud Security, (ii) E-mail Service and Security, (iii) Data Leak Prevention (DLP), and (iv) Backup Solution.	Work Order / Agreement Letter & Client Certificate	10
5	OEM Experience	OEM should have experience of supply and deployment cloud-based SSE solution of minimum 20000 users in single order for Government / Public Sector Unit (PSU) in India in last 3year. Marks shall be allotted as given below: 50000 users - 15 marks 30000 users - 10 marks 20000 users - 5 marks	Self-Declaration on OEMs letter head confirming no. of users in Government / PSU (Single order) in India. &	15

Sr. No.	Technical Parameters	Descriptions	Supporting Documents	Max. Marks
			Client Certificate, Copy of Work Order/ Agreement & Annexure VIII	
6	OEM Certifications	• SEI / CMMI- Process Level 3 or above • ISO 9001:2015 • ISO 27001:2013 for Information Security Management System • ISO/IEC 20000-1:2018 Marks shall be allotted as given below: • Any two of the above certifications – **3 marks** [where SEI/CMMI Process Level 3 is mandatory] • Every additional certification – **Additional 1 mark each**	Copies of Certificates with verifiable documentation including: • Certification Validity Confirmation • Link to Online Certificate Verification	5
7	Presentation	The sole bidder or consortium member's technical presentation showcasing at least the following: 1. Bidder's Capabilities 2. Understanding of Scope 3. Relevant Experience 4. Proposed Solution for MIDC 5. Approach and Methodology for MIDC 6. Migration Plan of existing email services 7. Project Management Methodology 8. SLA Management Framework	Requisite Presentation material	15
8	Demonstration	Demonstration of Product / Services features as requested by MIDC. Demonstration details will be shared during technical evaluation	Demonstration	15

All the bidders satisfying the above-mentioned parameters with cut off value of 80 Marks will be declared technically qualified for Commercial bid opening.

11. Commercial Evaluation Process

A) Total Bid Evaluation

a) Total Contract Value shall be calculated based on the format provided in Commercial Bid. The Total Contract Value (TCV) for each responsive bid shall be inclusive of all costs of necessary goods such as software license renewals, all taxes. etc. needed for the continued and proper operations of the system. (Refer Annexure XI for the commercial bid format)

a) Under QCBS selection, the technical bids will be allotted weightage of 80% (Eighty percent) while the commercial bids will be allotted weightages of 20% (Twenty percent).

b) The Bid with the lowest cost may be given a commercial score of 100 (one Hundred) and other proposals given commercial scores that are inversely proportional to their prices with respect to the lowest offer. Similarly, the Bid with the highest technical marks (as allotted by the evaluation committee) shall be given a score of 100 (one Hundred) and other proposals be given technical score that are proportional to their marks with respect to the highest technical marks.

c) The total score, both technical and commercial, shall be obtained by weighing the quality and cost scores and adding them up. Based on the combined weighted score for quality and cost, the bidders will be ranked in terms of the total score obtained.

d) The Bid obtaining the highest total combined score in evaluation of quality and cost will be ranked as H-1 followed by the bids securing lesser marks as H-2, H-3 etc.

e) The Bid securing the highest combined marks and ranked H-1 will be invited for negotiations, if required and shall be recommended for award of contract. In the event two or more bids have the same score in final ranking, the bid with highest technical score will be ranked as H-1 and will be invited first for negotiations.

f) An Evaluated Bid Score (B) will be calculated for each responsive Bid using the following formula, which permits a comprehensive assessment of the Bid price and the technical merits of each Bid:

$$\boldsymbol{Evaluated\ Bid\ Score\ (B)} = \left[\frac{C_{low}}{C} * 20\right] + \left[\frac{T}{T_{high}} * 80\right]$$

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

a) The Bid with the best evaluated Bid Score (B) among the responsive Bids shall be declared as the Most Advantageous Bid.

g) An Example demonstrating the calculation of evaluated Bid Score (B) is provided below:

Bidder	Technical Marks received by bidder	Commercial Quote by Bidder	Calculation of Evaluated Bid score	Evaluated Bid Score (B)	Rank
Bidder 1	88	110	$\left[\frac{110}{110} * 20\right] + \left[\frac{88}{95} * 80\right]$	94.105	H-2
Bidder 2	90	140	$\left[\frac{110}{140} * 20\right] + \left[\frac{90}{95} * 80\right]$	91.503	H-3
Bidder 3	80	160	$\left[\frac{110}{160} * 20\right] + \left[\frac{80}{95} * 80\right]$	81.118	H-4
Bidder 4	95	130	$\left[\frac{110}{130} * 20\right] + \left[\frac{95}{95} * 80\right]$	96.923	**H-1**

h) The bidder with the highest final score shall be treated as the Most Advantageous Bid. In the above example, Bidder 4 will be treated as the Most Advantageous Bid.

12. General Instructions for Financial Bid

a) Quantities indicated in the commercial bid format are indicative and may vary as per actual requirements. MIDC may add, drop, or replace any line item during the contract tenure as specified in the commercial bid format.

b) Payments will be made by MIDC against individual line items based on delivery and successful completion of the defined scope of work.

c) Payments shall be processed on a quarterly basis for each line item.

d) The quoted fees shall be inclusive of GST, Income Tax, duties, fees, levies, charges, commissions, and any other applicable taxes as per Indian laws. Any changes in applicable taxes will be accounted based on the actual tax rates prevailing on the date of billing.

A) Note to Bidders:

a) Bidders must upload only the 'Summary of the Commercial Format' on the e-Tendering portal.

b) Bidders are encouraged to visit the site and collect any additional information required, at their own cost and responsibility.

c) Bidders should quote rates after considering all costs necessary to fulfil the scope of work detailed in the bid document.

d) MIDC will constitute a Project Implementation Committee (PIC) to monitor the selected agency's performance and recommend payments accordingly.

e) Submission of only the 'Summary of the Commercial Format' on the e-Tendering portal is mandatory

f) Site visits for additional data are permitted at bidders' own cost and responsibility.

g) Any penalties or liquidated damages as specified under the Service Level Agreement (SLA) will be deducted from payments due to the selected agency.

h) MIDC reserves the right to scale up or scale down resources and to remove any line item at its discretion during the contract period.

i) All prices must be quoted exclusively in Indian Rupees (INR).

j) Quoted prices must be inclusive of all taxes, levies, duties, and applicable charges. A detailed breakup of applicable taxes, duties, and levies must be provided when requested. MIDC reserves the right to verify proof of payment for any such taxes or levies during billing/payment.

k) For the purpose of commercial evaluation, MIDC may apply standardized assumptions to reach a common bid price across all bidders. These assumptions shall not affect the actual contract value or payments made.

l) The contract price must remain firm and fixed throughout the contract duration and in the extension period if granted; no escalation of price or alteration of price will be accepted.

m) The selected agency is deemed to have satisfied themselves regarding the accuracy and sufficiency of the contract price, which shall cover all obligations under the contract without any additional claims.

n) Line items marked as Lump Sum in the BoQ will be treated as quantity one but bidders must quote a lump sum amount accordingly.

o) Payments will be made strictly for goods or services that have been delivered, installed, or operationally accepted as per the contract implementation schedule and at the unit prices specified in the commercial bid.

p) The total quoted bid price shall be considered the final amount for the purposes of commercial evaluation.

q) Quoted rates must cover all out-of-pocket and incidental expenses necessary to deliver the scope of work outlined in the RFP.

r) Rates must also account for all operational costs required to provide services as defined in the scope of work.

B) Additional Reminders:

a) Bidders should ensure all costs, taxes, and charges are accounted for in their bids to avoid future disputes or claims.

b) MIDC reserves the right to demand supporting documents for payments made towards taxes, duties, and levies during processing.

c) The contract price is binding and final; no price revisions will be entertained post-award unless otherwise specified.

13. Annexures

Annexure I – Bid Covering Letter

(To be submitted by the Bidder on the Company letterhead)

To,

The General Manager,
IT Cell, MIDC Udyog Sarathi,
Mahakali Caves Road,
Mumbai-400093.

Subject – Bid Response to Request for Proposal (RFP) for Selection of Agency for Implementing Cloud-based Enterprise Email Solution with Email Security, Data Protection and Backup Services for MIDC.

Reference: Tender bearing no. <Tender no.> published on <Publication Date>

Dear Sir/ Madam,

Having examined the RFP, the receipt of which is hereby duly acknowledged, we, the undersigned, offer to provide the professional services as required and outlined in the Request for Proposal (RFP) for "Selection of Agency for Implementing Cloud-based Enterprise Email Solution with Email Security, Data Protection and Backup Services for MIDC.".

We attach hereto our responses to pre-qualification requirements and commercial proposals as required by the RFP. We confirm that the information contained in these responses or any part thereof, including the exhibits, and other documents and instruments delivered or to be delivered to Maharashtra Industrial Development Corporation (MIDC), Maharashtra is true, accurate, verifiable, and complete. This response includes all information necessary to ensure that the statements therein do not in whole or in part mislead the department in its short-listing process.

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

We agree for unconditional acceptance of all the terms and conditions set out in the RFP document and agree to abide by this tender response for a period of 180 days from the date fixed for bid opening. We hereby declare that in case the contract is awarded to us, we shall submit the contract performance guarantee bond in the form prescribed the RFP.

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

We have read, and understood the content, T&C of this RFP. Through this letter, we certify our unconditional acceptance of the same and submit our bid response hereby.

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

_____

Signature of Authorized Signatory (with official seal)

Name	:
Designation	:
Address	:
Telephone & Fax	:
E-mail address	:
Date	:

Annexure II – Bidder's Particulars

(To be submitted by the Bidder on the Company letterhead)

Sr No	Description	Details (to be filled by the responder to the RFP)
1.	Name of the company	
2.	Official address	
3.	Phone No. and Fax No.	
4.	Corporate Headquarters Address	
5.	Type of Organization (Pvt. Ltd/ Public Ltd/ Proprietary etc.)	
6.	Website Address	
7.	Details of Company's Registration (Please enclose copy of the company registration document)	
8.	Name of Registration Authority	
9.	Registration Number and Year of Registration	
10.	CST/LST/VAT registration No.	
11.	Service Tax Registration No.	
12.	Permanent Account Number (PAN)	
13.	Company's Revenue for last 3 years (Year wise)	
14.	Company's Profitability for the last 3 years (Year wise)	
15.	Average Turnover for last three years (CA certified audited Statements to be submitted in company letter head with signature of authorized signatory)	
16.	GST Registration Number (with document evidence)	

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

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

Details	Authorized Signatory	Secondary Contact
Name		
Title		
Company Address		
Phone		
Mobile		
Fax		
E-mail		

Yours Sincerely,

_____

Signature of Authorized Signatory (with official seal)

Name :

Designation :

Address :

Telephone & Fax :

E-mail address :

Date :

Annexure III – Bidders Overall Turnover, Net-Worth for Last 3 Financial Years

<On the letterhead of the Chartered Accountant > <To be submitted along with Audited Financial Statements>

To,

The General Manager,
IT Cell, MIDC Udyog Sarathi,
Mahakali Caves Road,
Mumbai-400093.

Respected Sir/Madam,

I have carefully gone through the Terms & Conditions contained in the RFP Document with tender number <Tender no.> published on <Publication Date>, for Request for Proposal (RFP) for Selection of Agency for Implementing Cloud-based Enterprise Email Solution with Email Security, Data Protection and Backup Services for MIDC.

I have examined the books of accounts and other relevant records of <<Bidder>>. Based on such examination and according to the information and explanation given to us, and to the best of our knowledge & belief, we hereby certify that the annual turnover, Profit before Tax and Profit after tax for the three years i.e.

Sr No	Details	FY 2022-23 (In Lakhs)	FY 2023-24 (In Lakhs)	FY 2024-25 (In Lakhs)
1	**Annual Turnover**			
2	**Profit Before Tax**			
3	**Profit After Tax**			
4	**Average Annual Turnover**			
		(Signature of the Chartered Accountant)		

I further certify that I am competent officer in my company to make this declaration.

Yours Sincerely,

_____

Signature of Authorized Signatory (with official seal)

Name :

Designation :

Address :

Telephone & Fax :

E-mail address :

Date :

Annexure IV – Power of Attorney

To,

The General Manager,
IT Cell, MIDC Udyog Sarathi,
Mahakali Caves Road,
Mumbai-400093.

Dear Sir / Madam,

Subject – Power of attorney in response to Request for Proposal (RFP) for Selection of Agency for Implementing Cloud-based Enterprise Email Solution with Email Security, Data Protection and Backup Services for MIDC

Reference: Tender bearing no. <Tender no.> published on <Publication Date>

Know all men by these presents, we, (name of Firm and address of the registered office) do hereby constitute, nominate, appoint and authorize Mr / Ms..... son/daughter/wife and presently residing at....., who is presently employed with us and holding the position of ..... as our true and lawful attorney (hereinafter referred to as the "Authorized Representative") to do in our name and on our behalf, all such acts, deeds and things as are necessary or required in connection with or incidental to submission of our Proposal for "Request for Proposal (RFP) for Selection of Agency for Implementing Cloud-based Enterprise Email Solution with Email Security, Data Protection and Backup Services for MIDC**."** including but not limited to signing and submission of all applications, proposals and other documents and writings, participating in pre-bid and other conferences and providing information/ responses to the Authority, representing us in all matters before the Authority, signing and execution of all contracts and undertakings consequent to acceptance of our proposal and generally dealing with the Authority in all matters in connection with or relating to or arising out of our Proposal for the said Project and/or upon award thereof to us till the entering into of the Agreement with the Authority.

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

IN WITNESS WHEREOF WE, ...THE ABOVE-NAMED PRINCIPAL HAVE EXECUTED THIS POWER OF ATTORNEY ON THIS..... DAY OF ....., 20**

For.....

(Signature, name, designation, and address) Witnesses:

1.

2.

Notarized

Accepted

.....

(Signature, name, designation, and address of the Attorney)

Annexure V - Non-Blacklisting

(To be submitted by the Bidder as per the Documents Required in PQ/TQ Criteria)

To,

The General Manager,
IT Cell, MIDC Udyog Sarathi,
Mahakali Caves Road,
Mumbai-400093.

Dear Sir / Madam,

In response to the Tender Ref. No. _____ dated _____ for Selection of Agency for Implementing Cloud-based Enterprise Email Solution with Email Security, Data Protection and Backup Services for MIDC.

As an owner/ partner/ Director of _____, I/ We hereby declare that presently our Company/ firm _____is having unblemished record and is not declared ineligible for corrupt and fraudulent practices either indefinitely or for a particular period of time by any State/ Central Government/ PSU.

We further declare that presently our Company/ firm _____is not blacklisted and not declared ineligible for reasons other than corrupt and fraudulent practices by any State/ Central Government/ PSU on the date of Bid Submission.

If this declaration is found to be incorrect then without prejudice to any other action that may be taken, my/ our security may be forfeited in full and the tender if any to the extent accepted may be cancelled.

I further certify that I am competent officer in my company to make this declaration.

Yours Sincerely,

_____

Signature of Authorized Signatory (with official seal)

Name :

Designation :

Address :

Telephone & Fax :

E-mail address :

Date :

Annexure VI – Non-Withdrawal from projects

(To be submitted by the Bidder on the Company letterhead, as per the PQ criteria)

To,

The General Manager,

IT Cell, MIDC Udyog Sarathi,

Mahakali Caves Road,

Mumbai-400093.

Respected Sir,

In response to the Tender Ref. No. _____ dated _____ for Selection of Agency for Implementing Cloud-based Enterprise Email Solution with Email Security, Data Protection and Backup Services for MIDC, as an owner/ partner/ Director of _____, I/We hereby declare that we as a company have not withdrawn from similar government projects or terminated contract for similar project with Government entities (State Govt. / Central Govt./ ULBs/ other govt.) and other entities (public/private sector entities).

If this declaration is found to be incorrect then without prejudice to any other action that may be taken, my/ our security may be forfeited in full and the tender if any to the extent accepted may be cancelled.

I further certify that I am competent officer in my company to make this declaration.

Yours Sincerely,

_____

Signature of Authorized Signatory (with official seal)

Name :

Designation :

Address :

Telephone & Fax :

E-mail address :

Date :

Annexure VII - Checklist of Documents to be included in the Pre-Qualification Submission

Sr No	Pre-Qualification Criteria	Submitted (Yes/No/ NA)	Documentary Proof (Page No.)
1.	Scanned copy of payment slips of EMD & Tender Fee		
2.	EMD payment receipt generated from the e-tendering portal		
3.	Valid certification from bidders demonstrating their status as Micro and Small Enterprises (MSEs) in accordance with the MSE Procurement Policy issued by the Department.		
4.	Proof of Address		
5.	Certificate of Incorporation & Memorandum and Articles of Association of Bidder to be enclosed along with full address of Registered office. **OR** A partnership deed duly registered under the Partnership Act **OR** LLP firm registered certificate.		
6.	Copy of PAN card		
7.	Audited Balance sheet and Profit & Loss account statement of the Bidder for any of the last 3 audited financial years (FY 2022-2023, 2023-2024 and 2024-25)		
8.	Certificate duly signed by Statutory Auditor of the Bidder or Certified Chartered Accountant for average annual Turnover for last 3 financial years (FY 2022-2023, 2023-2024 and 2024-25)		
9.	Financial Audited balance sheets & Profit /loss statement, Statutory Auditor's Report, Notes to Accounts and Schedules forming part of accounts to be submitted.		
10.	Client Certificate, Copy of Work Order/ Agreement for similar projects experience of Email Solution in State / Central Government or Public Sector Unit (PSU)		
11.	Client Certificate, Copy of Work Order/ Agreement for similar projects experience. (Data Leak Prevention (DLP) / Backup Solution in State / Central Government or Public Sector Unit (PSU)		

Sr No	Pre-Qualification Criteria	Submitted (Yes/No/ NA)	Documentary Proof (Page No.)
12.	Client Certificate, Copy of Work Order/ Agreement for deployment of Cloud Security / Email Service component(s) in State / Central Government or Public Sector Unit (PSU)		
13.	Client Certificate, Copy of Work Order/ Agreement for OEM Experience Cloud SSE (Secure Service Edge) - OEM should have experience of supply and deployment cloud-based SSE solution of minimum 20000 users in single order for Government / Public Sector Unit (PSU) in India in last 3year.		
14.	Manufacturer's Authorization Form (MAF) for all solutions		
15.	Power of Attorney / Board Resolution to the authorized Signatory of the bid		
16.	Copy of GST certificate		
17.	Bidder’s Details (Refer Annexure II) & Data Security Declaration		
18.	Criteria related to Quality-of-Service Delivery - Copy of valid certificate issued to the Bidding Organization: ISO/IEC 9001:2015, or higher		
19.	Criteria related to Quality-of-Service Delivery - Copy of valid certificate issued to the Bidding Organization: ISO 27001:2013 or higher		
20.	Criteria related to IT Service Management Delivery - Copy of valid certificate issued to the Bidding Organization: ISO/IEC 20000-1:2018 or higher		
21.	Criteria related to Quality-of-Service Delivery - Copy of valid certificate issued to the Bidding Organization: (SEI) CMMI Level 3 or higher		
22.	Non-Blacklisting Self-Declaration from the authorized signatory of the bidder. (Refer Annexure V)		
23.	Non-Withdrawal: Self-Declaration from the authorized signatory of the bidder. (Refer Annexure VI)		
24.	Data Security Declaration (Refer Annexure XV)		

Annexure VIII - Details of Experience of Bidder in Various Projects

Sr. No.	Details of Experience of Bidder	
	Name of the Organization - <<Name of the Bidder that have executed / executing the project>>	
	Parameter	**Details**
General Information		
1.	Customer Name	
2.	Name of the contact person and contact details for the client of the assignment	
3.	Whether client visit can be organized	(YES / NO)
Project Details		
4.	Project Title	
5.	Start Date and End Date	
6.	Government/Private/PSU/Others please specify	
7.	Geographical Coverage (No. of locations the project covers)	
8.	Date of Go-Live	
9.	Total Cost of the project	
10.	Current Status (Live / completed / on-going / terminated / suspended)	
11.	No of staff provided by your company	
12.	Please indicate the current or the latest AMC period with the client *(From Month –Year to Month-Year)*	
13.	Please indicate whether the client is currently using the implemented solution	
Size of the project		
14.	Order Value of the project (in lakhs)	
15.	Capital Expenditure involved (in lakhs)	
16.	Cost of services provided by the bidder (in Lakhs)	

Sr. No.	**Details of Experience of Bidder**	
	Name of the Organization - <<Name of the Bidder that have executed / executing the project>>	
	Parameter	**Details**
17.	Cost of services provided by the partners if involved (in Lakhs)	
18.	Number of total users and concurrent users of the solution at the client location(s):	Total users
		Concurrent users
19.	Training responsibilities of Bidder	
20.	Any other information to be shared with MIDC	
Narrative Description of the Project:		
Detailed Description of actual services provided by Bidder:		
Documentary Proof: Copy of Work Order, Agreement and Client Certificate		
Highlights of the Key Result Areas expected and achieved		
List of modules and sub-modules implemented		

Note:

- Any citation that is submitted without the above form will not be considered for evaluation by MIDC.

It is the responsibility of the bidder to provide adequate documents against each citation. MIDC reserves the right to seek clarification or outrightly reject any citation that do not satisfy the qualification criteria as mentioned in the RFP. MIDC decision in this regard will be final and biding upon all the bidders.

Annexure IX - Checklist of Documents to be included in the Technical Qualification

Sr. No	Technical Qualification Criteria	Submitted (Yes/No)	Document Proof (Page No.)
1	Annual Turnover for last three financial years		
2.	Work Order / Agreement Letter along with Client Certificate demonstrating experience in supply / implementation of projects of Email solution in State / Central Government or Public Sector Unit (PSU) in last five years as on bid submission date		
3.	Work Order / Agreement Letter along with Client Certificate demonstrating experience in supply / implementation of project of Data Leak Prevention (DLP) / Backup Solution in State / Central Government or Public Sector Unit (PSU)		
4.	Work Order / Agreement Letter and Client Certificate evidencing experience of supply / implementation of Cloud security / email service for required project value in State / Central Government or Public Sector Unit (PSU) as on the date of bid submission		
5	Self-Declaration on OEMs letter head mentioning OEM experience of supply and deployment cloud-based SSE solution of minimum 20000 users in single order for Government / Public Sector Unit (PSU) in India in last 3 year.		
6.	Work Order / Agreement Letter and Client Certificate demonstrating OEM experience of supply and deployment cloud-based SSE solution of minimum 20000 users in single order for Government / Public Sector Unit (PSU) in India in last 3 year.		
7.	Certifications to be provided for the following industry standards related to Cloud email, data protection and backup service solution implementation: • SEI / CMMI – Process Level 3 or above • ISO 9001:2015 (Quality Management System) • ISO 27001:2013 (Information Security Management System) • ISO/IEC 20000-1:2018 (IT Service Management)		

Annexure X – Technical Specifications

1. Technical Specifications for cloud-based email solution

Sr No	Scope of Work	Summary	Compliance (Yes / No)
1	**Email as Service (Basic) – 1200 users**	● Up to 50 GB primary mailbox + Archival Space ● Compliance Archiving & advanced content discovery ● Email protection- Anti Spam and Anti Malware ● Full synchronization across mobile devices, tablets & web browsers. ● Collaboration Platform for chat, calls, and meetings with recording. ● The proposed OEM should be MeitY empanelled ● The proposed solution should have a provision to keep a copy of data in India as an when required ● Data in transit and rest should be encrypted ● Logs should be accessible in India	
2	**Email as Service (Standard) - 200 users**	● Up to 100 GB primary mailbox + Archival Space ● In-Place Hold & Litigation Hold: Preserves mailbox data for compliance or legal reasons. ● Auto-expanding archiving and management of inactive mailboxes. ● Email protection- Anti Spam and Anti Malware ● Full synchronization across mobile devices, tablets & web browsers. ● Collaboration Platform for chat, calls, and meetings with recording. ● The proposed OEM should be MeitY empanelled ● The proposed solution should have a provision to keep a copy of data in India as an when required ● Data in transit and rest should be encrypted ● Logs should be accessible in India	
3	**Email Collaborative Plan (Entry-Level) - 100 users**	● Up to 50 GB primary mailbox+ Archival Space ● Up to 1 TB cloud storage per user ● Compliance Archiving & advanced content discovery ● AI Features- inbuilt Generative AI tool with limited AI functionalities for users with Enterprise Data Protection. ● Email protection- Anti Spam and Anti Malware ● Collaboration & productivity enhancement features including web versions of office apps (word processing, spreadsheets, presentations), chat, meetings	

Sr No	Scope of Work	Summary	Compliance (Yes / No)
		● Collaboration Platform for chat, calls, and meetings with recording. ● The proposed OEM should be MeitY empanelled ● The proposed solution should have a provision to keep a copy of data in India as an when required ● Data in transit and rest should be encrypted ● Logs should be accessible in India	
4	**Email Collaborative Plan (Advanced) - 100 users**	● Up to 100 GB primary mailbox + Archival Space ● Up to 1 TB cloud storage per user ● Compliance Archiving, advanced content discovery, Legal hold ● Email Security features – Anti Spam and Anti Malware ● AI Features- inbuilt Generative AI tool with limited AI functionalities for users with Enterprise Data Protection. ● Collaboration & productivity enhancement features including web versions of office apps (word processing, spreadsheets, presentations), chat, meetings ● Collaboration Platform for chat, calls, and meetings with recording. ● The proposed OEM should be MeitY empanelled ● The proposed solution should have a provision to keep a copy of data in India as an when required ● Data in transit and rest should be encrypted ● Logs should be accessible in India	

2. Email Security

Sr. No	Features	Compliance (Yes / No)
1	The proposed solution must be compatible with all email services such as Microsoft 365, Microsoft Exchange, Google workspaces and more.	
2	The proposed solution must be able to create a direct connection with Microsoft 365 from the admin console, with no need for MX record redirections.	
3	The proposed solution must be able to use Microsoft APIs to create mail flow rules in the Microsoft 365 environment.	

Sr. No	Features	Compliance (Yes / No)
4	The proposed solution must alert customers of any configuration changes from the M365 console that could impact the email gateway mail flow setup and provide one-click resolution, restoration, and correction to configurations and mail flow.	
5	The proposed solution must protect and manage emails in the cloud through an intuitive cloud-based console, providing access to the entire range of vendor products through one interface, including web, endpoint, mobile, and server.	
6	The proposed solution must be able to create unique email security policies for individuals, groups or the whole domain.	
7	The proposed solution must have the option to clone an existing policy in the admin console.	
8	The proposed solution must provide admin access to end user allow and block lists with the capability to import, export, search, add, and delete entries directly from within the admin console.	
9	The proposed solution must be able to add Plain text and HTML disclaimer to outbound messages that can be configured through the Email Security policy in the admin console.	
10	The OEM should not be dependent on third party solutions, threat intel, Labs, research, Data Scientist, Threat Researchers or any other platform.	
11	The OEM should have a overall catch rate of 99.9% in a leading third comparative testing reports	
12	**Active Directory, Azure Active Directory and Google Directory Sync**	
13	The proposed solution must have the capability to synchronize with Microsoft Active Directory.	
14	The proposed solution must have the capability to synchronize with Microsoft Azure Active Directory.	
15	The proposed solution must be able to keep users automatically synchronized with the product using an Active Directory sync tool.	
16	The proposed solution must fully support automatic updating of AD data where businesses have completely moved to the cloud.	
17	The proposed solution must support Google Directory synchronization.	
18	The proposed solution must provide the administrator the capability to manually add mailboxes or import mailboxes and aliases when Active Directory is unavailable.	
19	**Self-service portal**	
20	The proposed solution must have a self-service portal for end-users.	

Sr. No	Features	Compliance (Yes / No)
21	The self-service portal must allow users to manage quarantined emails (accept/delete emails).	
22	The self-service portal must allow users to edit the allow/block rules.	
23	The self-service portal must allow users to view messages in the event of an outage using the emergency inbox.	
24	The end user portal must let users release emails on demand, and in-message quarantine digests provide a daily summary of quarantined mail, with the option to release direct from the inbox.	
25	**Business Continuity**	
26	The proposed solution must have email spooling that ensures no email is lost. In the event of a disruption to your Microsoft or Google Cloud email service, the product The proposed solution must have the capability to automatically queue the recipient's emails then deliver once the service is restored with a five day retry period.	
27	The proposed solution must provide read access to queued email from a 24/7 Emergency Inbox inside the end-user portal.	
28	The proposed solution must have the capability to send administrator alerts when mail can't be delivered to a server/service in the event of third-party cloud email service provider outages.	
29	**Protection from Spam and Malware**	
30	The proposed solution must have live threat updates to stop the latest attacks.	
31	The proposed solution must have anti-spam, anti-virus, and anti-phishing detection.	
32	The proposed solution must have reputation filtering that can block spam.	
33	The proposed solution must have next-generation reputation filtering technology that eliminates botnet spam at the IP connection level by monitoring connection requests and rejects those showing evidence of botnet connections.	
34	The proposed solution must protect against snowshoe spam.	
35	**Quarantine Summary Email**	
36	The solution should be able to access the M365's Quarantine emails list in the management console and also should be able to trigger the release or delete of these emails from Central and the action should be taken in M365.	
37	The proposed solution must be able to schedule when quarantine summary emails are sent to users.	

Sr. No	Features	Compliance (Yes / No)
38	The users be able to release or delete quarantined messages by clicking the appropriate link in the quarantine summary email.	
39	**Active Threat Protection**	
40	The proposed solution must have URL re-writing capability to check the website reputation of email links before delivery and at the time of click – blocking stealthy, delayed attacks.	
41	The proposed solution must have QR Code Scanning that scans messages for malicious URLs and QR codes that may lead to unsafe websites, malware, ransomware, or phishing sites when enabled.	
42	The proposed solution must have a cloud-based Sandbox that can detect both known and unknown malware and unwanted applications before it executes.	
43	The proposed solution must have the option to submit quarantined emails for cloud sandbox scanning through the admin console.	
44	**Post Delivery Protection**	
45	The proposed solution must be able to automatically remove messages containing attachments and URLs that are benign at the time of delivery but later become active and malicious.	
46	The proposed solution must have an 'on-demand clawback' feature that allows administrators to manually remove any message from users' inboxes with the click of a button in the admin console.	
47	When admins report a threat to the vendor's labs from the Message History report, it must have an option to 'clawback' the message from the user’s mailbox if the Post Delivery Protection (PDP) is configured in the account.	
48	When admins manually 'clawback' a message, it must have an option to specify the reason for the clawback as spam, malware, phishing, or unwanted email. Additionally, admins can report the message to the vendor's labs for analysis.	
49	The solution should allow administrators to connect their Google gateway domains for post-delivery protection. Post-delivery protection should automatically search and remediate messages delivered to users' inboxes that contain malicious URLs or attachments. It should also allow administrators to claw back objectionable or unwanted messages from users' inboxes on demand	
50	**Block Phishing Imposters**	
51	The proposed solution must use a combination of authentication techniques to identify and allow legitimate emails from trusted partners and block imposters.	

Sr. No	Features	Compliance (Yes / No)
52	The proposed solution must use Sender Policy Framework (SPF) to identify IP addresses authorized to send email from the domain.	
53	The proposed solution must use Domain Keys Identified Mail (DKIM) check to provide cryptographic proof that a message was sent from a specific sender and hasn't been tampered with.	
54	The proposed solution must use Domain Message Authentication Reporting & Conformance (DMARC) check to determine what to do when messages fail SPF or DKIM checks from the sender.	
55	The proposed solution must have Header anomaly detection to identify if the sender's display name is the same as one of your internal usernames.	
56	The proposed solution must be able to do an analysis of look-a-like domains to identify domain names similar to the corporate domain.	
57	Suspicious messages should have an option to be blocked, quarantined, tagged with a subject line warning, or have a banner added with a direct link to the user-level block list.	
58	The proposed solution must have an Allow and Blocked senders policy that allows administrators to restrict messages to or from specific email addresses, IP addresses, and domains, including support for wildcards, allowing you to block country-level TLDs.	
59	Smart Banners must allow end users to update their personalized allow and block sender lists from within the email itself, while the Self-Service Portal allows these lists to be managed.	
60	The solution should inform the user via a banner if the user has not received an email from the sender address before.	
61	**Impersonation Protection**	
62	The proposed solution must be able to detect messages that pretend to be from well-known brands, very important people (VIPs) in your organization, or your vendor, customer, or partner organizations.	
63	The proposed solution must be able to Protect External VIPs. This protects your users from email attacks impersonating not only your internal VIPs, but also individuals from your vendor, customer, and partner organizations.	
64	The proposed solution must have an option to add these 'External VIPs' to your list of VIPs to detect and flag emails that try to impersonate these important individuals.	

Sr. No	Features	Compliance (Yes / No)
65	The proposed solution must have a VIP management list that can contain a minimum of 500 email addresses (Internal and External VIPs).	
66	The proposed solution must be able to import and export VIP list.	
67	The proposed solution must have a VIP Impersonation option that detects emails attempting to impersonate high-profile individuals within your organization (internal VIPs) or trusted external contacts, such as vendors, customers, or partners (external VIPs) when enabled.	
68	VIP Impersonation must detect emails without an exact name match.	
69	VIP Impersonation must have an Aggressive Mode option that detects emails solely based on VIP name matches, including fuzzy name variations, without relying on machine learning or heuristics.	
70	The proposed solution must have a Brand Impersonation option that detects emails attempting to spoof frequently targeted brands or domains. This setting helps prevent impersonation of well-known organizations.	
71	The proposed solution must have a General Impersonation option that detects emails that don't match VIP names or frequently targeted brands but are still considered impersonation attempts based on machine learning and anti-phishing heuristics.	
72	**Account Compromise**	
73	The proposed solution must have an Account Compromise setting that helps admins detect when a user's account may be compromised. The proposed solution must allow admins to configure email notifications to alert administrators or key users as soon as the vendor flags suspicious activity. This allows them to respond quickly and help prevent a major security breach.	
74	The vendor platform must monitor email activity to detect unusual behavior that may indicate a compromised account. For example, it flags the activity if a user suddenly sends an unusually high volume of emails or shows patterns that differ from their normal behavior. It then notifies the recipients you've configured.	
75	**Geo IP Protection**	
76	The proposed solution must be able to select the countries from which you want to disallow messages.	
77	**Bounce Address Tag Validation (BATV) Protection**	

Sr. No	Features	Compliance (Yes / No)
78	The proposed solution must have an option that tags outbound messages so that in the event of a bounce, its tag can be validated to determine whether the bounce message is valid. The proposed solution must allow admins to configure an action for invalid bounce messages to safeguard users from being targeted by backscatter attacks.	
79	**Data Loss Prevention**	
80	The Data Control policy must allow admins to configure a rule to search in the email subject, message body, attachment name, attachment content, or any combination of those message parts.	
81	The proposed solution must be able to create multi-rule Data Control policies for groups and individual users to ensure protection of sensitive information with discovery of financials, confidential contents, health information, and PII in all emails and attachments.	
82	The proposed solution must be able to create custom Content Control Lists (CCL) using the vendor's CCLs or customize out-of-the-box templates for specific CCLs.	
83	The proposed solution must have granular control of data breach prevention policies, including multi-rule policies for groups and individual users with seamless integration of encryption	
84	The solution should scan images for illicit content in incoming and outgoing email, and educate offending users, including QR code scanning for redirection to phishing sites if needed in future.	
85	The proposed solution must have a single console, managing data loss prevention for email, alongside next-gen endpoint protection	
86	The proposed solution must be able to inspect the attributes of any email by using the Message Attribute rule in the Data Control policy	
87	The Data Control policy must have a Message Attributes option that allows admins to filter messages by header, source, and size.	
88	The Data Control policy must have a Modify Header action with the following options: • Add header – inserts a new header and value in the message • Edit header value – edits values of all matching headers • Strip header – strips all matching headers	
89	Data Control rules must allow admins to add and change email headers to select how a message is encrypted.	

Sr. No	Features	Compliance (Yes / No)
90	The Data Control rule must be able to add the following headers and change the way the encryption is applied to the messages that match the rule's criteria:	
91	Should support Portal encryption without recipient authentication where in the recipient will receive a link to the portal-encrypted email, which will not require authentication to view the message if this header is set to true.	
92	Admins must be able to set a message expiry period up to the maximum set in the account. The default maximum expiry period is 30 days, which administrators may have modified as part of the account's custom branding.	
93	The sender must receive a notification when the encrypted email is sent to the recipient if this header is set to true.	
94	The sender must receive a notification when the recipient reads the encrypted email if this header is set to true. In the case of Push Encryption, the read notification must only be sent for the registration message.	
95	The admin console must allow admins to strip, re-attach or download attachments from quarantined emails.	
96	**Email Encryption**	
97	The proposed solution must give users the capability to encrypt emails using the product's M365 add-in.	
98	The proposed solution must have push-based encryption that protects the entire email or attachments only.	
99	The proposed solution must have enforced TLS encryption that prevents eavesdropping when messages are in transit.	
100	The proposed solution must be able to add a digital signature to verify sender identity with S/MIME.	
101	The proposed solution must have an optional full web portal encryption (requires an add-on license) that allows users to manage, read, and reply to encrypted messages in a secure web portal.	
102	The proposed solution must be able to customize the branding of your encryption portal and encrypted messages with your organization's logo and colors (requires an add-on license) in the same console	

Sr. No	Features	Compliance (Yes / No)
103	The solution must support DMARC Manager features that gives domain owners clear visibility into how their domains are used in outbound email in the same console, if needed in future with an additional cost. Some features it should support: 1. Should aggregate reports and files that must include information on the authentication status of messages delivered on behalf of a domain. They must show which sources are sending on your behalf and how their messages were evaluated against your DMARC policy. 2. Must support CNAME-based DNS validation 3. Must support BIMI management, TLS-RPT, and MTA-STS record hosting and management. 4. Must help enforce DMARC conformance and compliance through reporting, DNS record management, and process automation. 5. Must verify the identity of senders, ensuring that emails received are from the trusted source they claim to be.	
104	**Comprehensive Reporting**	
105	The solution should allow administrators to specify mailboxes or distribution lists to receive a copy of any message reported by administrators. This feature should provide visibility into messages reported as false positives (clean) or false negatives (threats).	
106	The proposed solution must provide statistics reports within the console in the form of tables and graphs with custom date ranges.	
107	The proposed solution must have the following reports available:	
108	Shows logs of all mail processed by the system, including visibility into messages rejected because their TLS did not meet the requirements of the Secure Message Policy. Also has an option to filter messages by their category, status, and TLS encryption applied. Also shows inbound messages that were rejected because the recipient mailbox wasn't found.	
109	Shows a summary of all emails and includes a statistical report about the number of emails transported inbound and outbound over TLS v1.3, TLS v1.2, and unencrypted.	
110	Shows a summary of inbound messages that were analyzed for threats using static and dynamic analyses. The report gives verdicts for both types of submissions – the	

Sr. No	Features	Compliance (Yes / No)
	messages reported as threat (false negative detection) and the messages reported as clean (false positive detection).	
111	Volume of blocked, warned, and allowed URLs.	
112	Shows a report of all messages logged by the data control policy.	
113	Summary of M365 messages removed post-delivery.	
114	Should provide license Usage Summary	
115	The proposed solution must have an API that can query message history information from the vendor Data Lake using the admin console	
116	The proposed solution must have an API that lets admins manage mailboxes such as create, read (or find), update, and delete mailboxes in the email protection solution.	
117	**Phishing Simulation & Training**	
118	The proposed solution must be able to emulate a range of phishing attack types to help you identify areas of weakness in your organization's security posture and empower users through engaging training to strengthen your organization's defenses.	
119	The proposed solution must have over 500 customizable, realistic and challenging phishing attacks.	
120	Email simulations must support min 3 languages:	
121	English	
122	Hindi	
123	Marathi	
124	Campaigns should have the following template categories:	
125	a. Phishing: This simulates a phishing attack against your users. It encourages your users to click a link in an email.	
126	b. Credential Harvesting: This simulates an attack designed to obtain login ids and passwords. It encourages your users to enter credentials into a fake website. No passwords are collected.	
127	c. Attachment: This simulates an attack designed to deploy malicious attachments on your system. It encourages your users to open an attachment in an email.	
128	d. Training: This allows you to send anti-phishing training to your users without a simulated attack.	

Sr. No	Features	Compliance (Yes / No)
129	Baseline testing (attack simulation without training) in campaigns should be available.	
130	The proposed solution must have the capability to create randomized attacks by allowing admins to select up to five phishing email templates when building a campaign. These emails should then be randomly distributed across the selected users and provide administrators insight into each user's susceptibility to future attacks.	
131	**Training**	
132	The proposed solution must have over 100 interactive training modules that will educate users about specific threats, such as suspicious emails, credential harvesting, password strength, and regulatory compliance.	
133	Training materials must support 3 languages:	
134	English	
135	Hindi	
136	Marathi	
137	Training campaigns without attack simulation should be available.	
138	The proposed solution must have the option to redirect caught users to your own hosted training material.	
139	**Customization and Scheduling**	
140	The proposed solution must have Email Template User Variables	
141	The proposed solution must have Training Reminder Emails	
142	The proposed solution must have customizable Landing Pages	
143	The proposed solution must have Immediate or Scheduled Campaign Broadcast options	
144	The proposed solution must have the capability to conduct Distributed Broadcast across user list	
145	**Reporting and Management**	
146	The proposed solution must have an Outlook add-in that enables users to report suspected phishing and spam messages with one click right from within Outlook.	
147	The Outlook Add-in should work for Office 365 Business subscription (Exchange online) mail accounts.	

Sr. No	Features	Compliance (Yes / No)
148	The solution dashboard should provide at-a-glance campaign results on user susceptibility and allows you to measure overall risk levels across your entire user group with live Awareness Factor data, including:	
149	Top level campaign results	
150	Organizational trend of caught employees and reporters	
151	Total users caught	
152	Testing coverage	
153	Days since last campaign	
154	Drill–down reports should give deeper insight into performance at an organizational or individual user level.	
155	Reports must have an option to export to a CSV file.	
156	The solution should be easy to use and can be easily accessed on any supported browser.	
157	Must have an option to import users manually, from Active Directory or from a CSV file.	
158	Should have a section that lists the domains and IP addresses that the solution uses to send campaign emails.	
159	Should have an automated report on phishing and training results	

3. Advanced Classification, Endpoint, Web and Email DLP

Sr. No	Technical Specifications	Compliance (Yes / No)
160	Solution should be delivered through cloud service edge of the solution vendor, and the actual data processing cloud service edges must in India to ensure no actual data of customer leaving India geography for processing or storage.	
161	The proposed Secure Internet solution must be cloud native platform and the OEM should have services hosted in at least 7 own / co-located/ MeitY-empaneled cloud service provider's data centers in India with local compute.	
162	The solution provider should have achieved DoD Impact Level 5 (IL5) and FedRAMP High Authorization to reflect better security standards. The offered solution must be certified with CSA STAR, Fed Ramp, ISO 27001, ISO 27017, ISO 27018, SOC2, SCO3 certification and Zero Trust Architecture designed by NIST (National Institute of Standards and Technology).	

Sr. No	Technical Specifications	Compliance (Yes / No)
163	The location of Cloud server should be in India and data should be stored in India only.	
164	All the feature functionalities listed in technical specification must be available from Day-1	
165	The endpoint agent of the proposed zero trust should have a packet capture capability as a built-in feature for ease of troubleshooting with a better user experience. In case this is not available as a built-in feature, bidders can include additional packet capture tools in their solution for the user endpoints with the required license, support, and services and the tool needs to be tightly integrated with the SSE endpoint agent to deliver the mentioned functionality. To ensure security best practices are followed, the bidder must avoid using freeware tools and ensure proper patching and upgrades of the provided packet capture tool.	
166	The solution must capture detailed device details like device name, hostname, model, OS type, version and allow creation of device/device group-based policies. The device posture check functionality of the zero-trust platform must support minimum 19 different predefined conditions to allow an administrator to define business relevant conditions for different device types. The conditions much include validating the Certificate Trust, File Path, Registry Key, Client Certificate, Domain Joined, Process Check, firewall, Encryption, Detect Antivirus along with AV signature update, OS Version, etc.	
167	The solution must operate in a full-proxy architecture (Hide user and application IP address) and should perform 100% SSL inspection of the internet traffic at scale without performance degradation	
168	Solution architecture should be designed in such a way that actual data should not leave India geography and hence should be processed in India based Data Centers only	
169	Solution architecture should ensure that actual data should not be stored temporarily or permanently in vendors' cloud service edge irrespective of file type and file size	
170	The solution should have a unified singular agent delivering all the critical services like Data Protection, Internet Security, ZTNA, Digital Experience Monitoring, active defense	
171	All the required functionalities should be delivered through single endpoint agent for endpoint data protection, data discovery and classification	

Sr. No	Technical Specifications	Compliance (Yes / No)
172	To avoid DLP policy exception and continuous access to critical SaaS applications during disaster scenarios when cloud service edge is not reachable/available, the solution providing vendor must provide disaster recovery for the critical applications to ensure authenticated users continue to have access to these applications even when there is a global outage in the vendor's cloud.	
173	all the required functionalities should be delivered through single endpoint agent for endpoint data protection, data discovery and classification	
174	Solution should be able to provide an automated data discovery report highlighting SaaS apps / websites are getting accessed by users	
175	Solution should be able to categorize such apps into risky / non-risky depending on various security parameters	
176	Solution should be able to provide a consolidated SaaS dashboard highlighting number of SaaS apps accessed, sanctioned / unsanctioned status of these apps, amount of data uploaded / downloaded along with relevant logs	
177	all the required functionalities should be delivered through single endpoint agent for endpoint data protection, data discovery and classification	
178	Solution should be able to identify any data exfiltration/leakage through images and screenshots	
179	Solution should allow to create DLP policies based on keywords , regex patterns, Labels , fingerprinting as well as in-built ML (Machine Learning) dictionaries	
180	Solution should allow to create DLP policies based on user, user groups, departments, risk score, file size, file extensions etc.	
181	Inline Web DLP should operate in an browser agnostic environment (no dependency on web browser or its version)	
182	Solution should be able to inspect all web traffic like http / https and FTP and provide granular DLP inspection controls	
183	Inline DLP should be able to support file size up to 400 MB for content scanning / fingerprinting etc. without storing in any of the solution component	
184	Solution should be able to detect and block Encrypted/Password-Protected Files	
185	Solution should have ability to distinguish between corporate and personal instances of Outlook, OneDrive, SharePoint, MS Teams and apply granular DLP controls accordingly	

Sr. No	Technical Specifications	Compliance (Yes / No)
186	Solution should be able to provide granular controls over SaaS apps like Gmail , Facebook, LinkedIn etc. in terms of blocking posts, blocking file attachments, chats etc. and doing content based DLP inspection	
187	The Solution should provide the Flexibility of setting up customer notification template for violations	
188	The Solution must provide a way to send attachment of the violating content to the DLP Administrators	
189	The Solution must provide Alerting Mechanism for identifying User Anomalies such as Bulk Data Transfer, Impossible Travel, Failed Logins etc.	
190	Solution should be able to block & monitor emails containing sensitive data in email subject, email body and email attachment sent to external domains, to personal email accounts from Gmail, Yahoo etc., to competitors, or to specific recipients	
191	Per user email policy enforcement; meaning not all recipients will be blocked when only some of the recipients in the same email matches an email policy.	
192	Email DLP solution should be able to apply granular dlp controls basis per email recipient or email domain (rather than doing a blanket allow / block)	
193	Solution should be able to provide email DLP functionality without any dependency and deployment of mail transfer agent or co-existence with mail transfer agent or making any changes in MX records	
194	The Solution must be able to Monitor, Block, Quarantine Sensitive Emails and Attachments as per Pre-defined and Custom Classifiers [for e.g. PII]	
195	The Solution must be able to Scan Email Body and Attachments for leakages	
196	Endpoint DLP should support and protect Bluetooth, printing, network share channel.	
197	Solution should offer monitor, block and justification ability for endpoint (user system) sensitive data movement through printers including print-to-pdf	
198	Solution must be able to apply Granular Tenancy Restriction based on classification of document [PII, PCI, PHI etc.]	
199	Endpoint DLP should allow data to be transferred to only authorized USB's	
200	Endpoint DLP should be able to protect / encrypt sensitive files copied to USB drive so that the protected data is accessible from customer managed devices only.	
201	Endpoint DLP should offer preventive actions like monitor, block and justification of sensitive data movement across network shares	
202	Endpoint DLP should be able to protect / encrypt sensitive files copied to USB drive so that the protected data is accessible from customer managed devices only.	

Sr. No	Technical Specifications	Compliance (Yes / No)
203	Endpoint DLP solution should monitor & block sensitive data as well as ask justification of sensitive data movement across USBs	
204	Endpoint DLP's preventive actions like monitor, block and justification of sensitive data movement should be applicable across personal sync clients such as Dropbox, box, google drive, one Drive, iCloud etc.	
205	Endpoint DLP should allow customized End user notifications for different endpoint channels like block for print, monitor for N/w shares, Justify for sync clients etc.	
206	Endpoint DLP should perform data discovery on endpoints without any manual configuration	
207	Endpoint DLP should list all the activities performed on the endpoint without any policy configuration so that data flow can be benchmarked and policies can be designed to address false positive, to minimize resistance from users and to justify DLP policies	
208	Solution should be able to control hardware devices like USB and Printers by creating granular policies based on device type, vendor ID, user, department etc.	
209	Automated visibility on device inventory if any hardware device such as USB / Printer is plugged into any enterprise endpoint	
210	Endpoint DLP Controls like allowing approved USBs, content scanning, OCR for images/screenshots etc. must function when user machine is in offline mode meaning have no internet connectivity.	
211	Endpoint DLP solution should auto pull inventory attached to the endpoint	
212	Endpoint DLP must list all the applications running on the endpoint along with their associated risk levels	
213	Endpoint DLP should provide time-based exceptions on endpoint which gets auto revoked post expiry of duration	
214	The solution must provide User Coaching when any user performs Sensitive Data Transfer	
215	The Solution must support End Point DLP for Windows and MACOS Operating Systems	
216	Endpoint DLP should allow read only from USB disk drive.	
217	Provides device control (i.e.. No need to check for file content) to block usage of removable storage, printers or Bluetooth.	
218	Support Unicode (non-English) and ShiftJIS (specific Japanese character support) encoding.	

Sr. No	Technical Specifications	Compliance (Yes / No)
219	Solution should support where User can request for exemption from endpoint DLP rule enforcement for limited time period by entering a OTP.	
220	Endpoint DLP should Inspect content of file when copying to thick client on the laptop. Examples of thick clients are WhatsApp, WinSCP, GDrive and OneDrive. The objective is to provide coverage where the cloud proxy is unable to perform the inspection because it is not in the traffic path or the traffic is not using the common data in motion encryption.	
221	Endpoint DLP is able to define custom thick client by their process name, including their Original File Name (to prevent file name tampering).	
222	Endpoint DLP should inspect content of a paste (i.e.. clipboard) when copying sensitive context to thick client on the laptop. Examples of thick clients are WhatsApp, WinSCP, Gdrive and OneDrive. The objective is to provide coverage where the cloud proxy is unable to perform the inspection because it is not in the traffic path or the traffic is not using the common data in motion encryption.	

4. Backup – Email and Endpoint

Sr. No.	Endpoints Backup	Compliance (Yes /No)
223	The proposed Backup Solution should provide feature for End User Profile Backup. The proposed Email and Endpoint should be from same OEM.	
224	The proposed Backup Solution should provide feature for Legal hold capabilities for data preservation/retention and collections	
225	The proposed Backup Solution should provide feature for PC Settings Migration (USMT integration)	
226	The proposed Backup Solution should provide feature for Centralized Web based interface for administrative actions	
227	The proposed OEM should have capability to provide Unlimited storage for End User Backup and MIDC should able to add user-based backup with unlimited storage for future use at same price of email backup per user cost mentioned in RFP	
228	The proposed Backup Solution should provide feature for de-duplication across devices	
229	The proposed Backup Solution should provide feature for Local Cache on device (allows for offline backups and rapid restore capabilities)	

Sr. No.	Endpoints Backup	Compliance (Yes /No)
230	The proposed Backup Solution should provide feature for Branch Office Cache (time-shifting upload options and rapid restore)	
231	The proposed OEM should provide feature for Capacity and Device based licensing	
232	The proposed Backup Solution should provide option for Bandwidth management	
233	The proposed solution OEM solution should be hosted on MeitY Empanlled DC	
234	The proposed Backup Solution should provide feature for LDAP integration for user management	
235	The proposed Backup Solution should provide feature for Single sign-on	
236	The proposed Backup Solution should provide feature for Option for Unlimited retention of versions	
237	The proposed Backup Solution should provide feature for Forever keeping older versions (Number of days of version history to be retained for individual files)	
238	The proposed Backup Solution should provide feature for Forever Retaining deleted files	
239	The proposed Backup Solution should provide feature for End user self-restore portal	
240	The proposed Backup Solution should provide feature for Option to configure Backup frequency to 1 minute	
241	The proposed Backup Solution should provide feature for Frequency based backup for Endpoint	
242	The proposed Backup Solution should provide feature for Scheduled based backup	
243	The proposed Backup Solution should be ISO 27001, HIPAA, FERPA, GLBA, and GDPR compliant	
244	The proposed Backup Solution should have Role based Access control	
245	OEM should directly provide post-sales support	
246	The proposed OEM should provide 99.9% uptime	
247	The proposed solution should have export option to onsite storage	
248	The proposed solution should have in-transit and at-rest encryption	
249	Should have Device Deletion	
250	Should have an option to setup maximum upload or download limit	
251	Should have an option to set maximum backup quota for users	
252	Should be agent based to ensure remote and travelling users endpoint device should get backed up without needing to connect to office network	
253	Should have efficient deduplication of encrypted data to optimize storage	

Sr. No.	Endpoints Backup	Compliance (Yes /No)
254	Should operate in a control framework based on adherence to SOC 2 Type 2 standards	
	Backup Solution - Email	
255	Proposed Backup Solution Provider Should Provide Option for Backup Solution like Microsoft 365 services (Exchange, OneDrive, SharePoint, Teams), Google Workspace (Email, Google Drive) or any proposed email solution.	
256	Proposed Backup Solution Provider Should Provide Feature for Centralized Web based interface for user management and administrative actions	
257	Proposed Backup Solution Provider Should Provide Option for Permission-only restore	
258	Proposed Backup Solution Provider Should Provide Option for User Self Data Restore	
259	Proposed Backup Solution Provider Should Provide Option for Unlimited Retention	
260	Proposed Backup Solution Provider Should Provide Option for Unlimited Storage	
261	Proposed Backup Solution Provider Should Provide Option for IP restrictions on access	
262	Proposed Backup Solution Provider Should Provide Option for Restore to point in time	
263	Proposed Backup Solution Provider Should Provide Option for Geo-sovereignty	
264	Proposed Backup Solution Provider Should Provide Option for Agentless backup (nothing on prem)	
265	Proposed Backup Solution Provider Should Provide Option for Auto-discovery	
266	Proposed Backup Solution Provider Should Provide Option for Auto-scaling to onboard new customers	
267	Should have DC in India	
268	Should have MeitY empanlled DC	
269	Should have post-sales support from direct license provider (OEM)	
270	Should have 99.9% uptime	
271	Should have export option to onsite storage	
272	Should have in-transit and at-rest encryption	
273	Should have an option to trigger manual backup for maintenance failsafe	
274	Should have automated backup of Once or Thrice a day	
275	Should have an option to pause or stop the backup for selected users	
276	Should be ISO27001, HIPPA and GDPR compliant	

Sr. No.	Endpoints Backup	Compliance (Yes /No)
277	Should be certified by Microsoft and Google for backup	
278	Should have integration for 2FA, OAuth Access, SAML/OCTA integration	
279	Should have Role based Access control	
280	Should support multi-admin access with fine-grained access management per admin.	
281	Should be able to restrict backup/restore requests to company-approved IP addresses.	
282	Should Provide Export options: PST (Exchange), ZIP/native file (OneDrive/SharePoint).	
283	Should Provide Incremental/Differential backups with change tracking.	
284	Should Provide Backup of permissions, metadata, sharing settings.	
285	Should Provide Backup of Teams structure (files, conversations, channels, tabs).	
286	Should Provide Point-in-time restore.	
287	Should Provide Restore to original or alternate location; cross-user restore.	

5. Email Phishing Stimulation

Sr. No.	Technical Specifications	Compliance (Yes / No)
288	The proposed solution should be bundled with overall solution and to be provided to MIDC without any additional cost. The solution shall be a web-based phishing simulation platform deployed within customer-owned infrastructure / Cloud Environment	
289	The proposed solution should be perpetual license with support for 2 years from OEM with updates. The solution should support unlimited user and unlimited campaigns	
290	The solution must support on-premises and private cloud deployment without dependency on external SaaS services.	
291	The solution should support deployment on Windows Server / RHEL / Free Linux (e.g. Ubuntu) operating systems	
292	The proposed solution can be deployed on Virtual Machine and containerized deployment using Docker.	

Sr. No.	Technical Specifications	Compliance (Yes / No)
293	The solution shall consist of the following components: Web-based Administration Console Campaign Management Engine Landing Page Hosting Service REST API Service Backend Database	
294	The solution shall support deployment behind reverse proxy / load balance	
295	The solution shall support multiple administrative users.	
296	The solution shall provide role-based access control (RBAC).	
297	The solution shall support integration with LDAP / Active Directory.	
298	The solution shall support creation, scheduling, execution, and closure of phishing campaigns.	
299	The solution shall support multiple concurrent phishing campaigns.	
300	The solution shall allow pause, resume, and stop of campaigns.	
301	The solution shall support target user grouping and segmentation.	
302	The solution shall support customizable phishing email templates using HTML and text formats.	
303	The solution shall support dynamic placeholders (e.g. username, email ID, department).	
304	The solution shall support attachment-based phishing simulations.	
305	The solution shall integrate with external SMTP relays.	
306	The solution shall support SMTP authentication and TLS encryption.	
307	The solution shall not include or mandate an internal mail server.	
308	The solution shall support custom phishing landing pages.	
309	Landing pages shall be hosted over HTTPS using customer-provided TLS certificates.	
310	The solution shall track the following user actions: Email open, Link click, Credential submission	
311	The solution shall support post-click redirection to awareness pages.	
312	The solution shall provide campaign-wise and user-wise reports.	
313	The solution shall provide metrics including Emails sent, Emails opened, Links clicked, Credentials submitted	
314	The solution shall support export of reports in CSV and JSON formats.	
315	The solution shall maintain historical campaign data for trend analysis.	

Sr. No.	Technical Specifications	Compliance (Yes / No)
316	The solution shall expose RESTful APIs for automation.	
317	The APIs shall support: Campaign creation, User and group management, Report extraction	
318	API communication shall be over HTTPS using token-based authentication.	
319	The solution shall support an embedded database for small deployments.	
320	The solution shall support opens source database (e.g. MySQL / MariaDB)	
321	The solution shall generate audit logs for: User login, Administrative actions, Campaign modifications	
322	Logs shall be exportable or forwardable to external SIEM platform	
323	The bidder shall provide: Installation Guide Administrator Manual API Documentation Security Hardening Guide	

Annexure XI – Format for Commercial Proposal and Instructions

(To be submitted by the Bidder on the Company letterhead and in the BoQ excel-sheet or commercial bid excel-sheet available on tendering site with this RFP)

To,

The General Manager,
IT Cell, MIDC Udyog Sarathi,
Mahakali Caves Road,
Mumbai-400093.

Subject – Commercial Proposal in response to Request for Proposal (RFP) for Selection of Agency for Implementing Cloud-based Enterprise Email Solution with Email Security, Data Protection and Backup Services for MIDC.

Reference: Tender bearing no. <Tender no.> published on <Publication Date>

Respected Sir / Madam,
I / We undertake that the prices are in conformity with the requirement as specified in this RFP. We will charge the department for this project as mentioned below:

Sr. No.	Description	Unit Type	Quantity	Yearly Cost (in Rs)	Total Cost for 2 Years (Excl. GST)
A. Licence subscription cost					
1.01	Email Solution – Type 1 Basic (50 GB)	NOS	1200		
1.02	Email Solution – Type 2 Basic (100 GB)	NOS	100		
1.03	Email Solution – Type 3 Advance (50 GB)	NOS	100		
1.04	Email Solution – Type 4 Advance (100 GB)	NOS	100		
1.05	Email Security	NOS	1500		
1.06	Data Protection – Email	NOS	1500		
1.07	Data Protection – Endpoint	NOS	2000		
1.08	Backup – Endpoint (20 TB)	NOS	2000		
1.09	Backup – Email	NOS	1500		
A	**Total cost (INR)**				

Sr. No.	Description	Unit Type	Quantity	Yearly Cost (in Rs)	Total Cost for 2 Years (Excl. GST)
B. One Time Cost					
2.01	Migration of Existing Emails if applicable	NOS	1	NA	
B	**Total Cost for Migration (INR)**				
C. Operation & Maintenance					
3.01	Operation and Maintenance Cost	NOS	1		
D= A+B +C	**Total Contract Value (INR)**				

Note:

1. Payments shall be made by the Agency as per the terms and conditions of the Tender Documents.
2. The Total Contract Value shall be firm and not subject to any alteration.
3. No column has been left blank otherwise our bid shall be rejected.
4. All the prices are entered in Indian Rupees Only.
5. Prices indicated in the schedules are inclusive of all taxes, Levies, duties etc. We have provided breakup of all Taxes, Duties and Levies wherever asked for.
6. During the payment stage, Department reserves the right to ask us to submit proof of payment against any of the taxes, duties, levies indicated.
7. The Bidder shall quote at special discounted rate for all items listed in the Annexure XI – Format for Commercial Proposal, given that the contract term is of two (2) years plus one (1) year of extension if granted, and should be lower than the rates published on their official websites

I further certify that I am competent officer in my company to make this declaration and specify commercial proposal details given here.

Yours Sincerely,

_____

Signature of Authorized Signatory (with official seal)

Name :

Designation :

Address :

Telephone & Fax :

E-mail address :

Date :

Annexure XII – Format for Submission of Pre-Bid Queries

All enquiries from the bidders relating to this RFP must be submitted on email ID mentioned in Bid Control Sheet in the following format:

- **Name of Bidder:**
- **Name and position of person submitting queries:**
- **Full formal address of the organization including phone, fax, and email id:**

Sl. No.	RFP Document Reference (Page No.)	Content of the RFP requiring clarification	Clarification Sought
1			
2			

Annexure XIII - Format for Performance Bank Guarantee

(To be submitted on Rs. 500/- (five hundred) non-judicial stamp paper)

Bank Guarantee No. _____ dated _____

The General Manager,
IT Cell,
MIDC Udyog Sarathi,
Mahakali Caves Road,
Mumbai-400093

Dear Sir/ Madam,

In consideration of Maharashtra Industrial Development Corporation (MIDC) having agreed to exempt, M/s_____ having its registered / principal office at _____ [hereinafter referred to as ‘‘**Selected Agency’’** which expression unless repugnant to the context and meaning thereof shall include its success and assigns], from depositing with **Maharashtra Industrial Development Corporation (MIDC)** a sum of Rs._____ towards security / performance guarantee in lieu of the said **‘‘Selected Agency’’** having agreed to furnish an irrevocable bank guarantee for the said sum of Rs. _____ as required under the terms and conditions of Contract / Work Order / Purchase Order no. _____ dated _____ [hereinafter referred as the ‘Order’] placed by Maharashtra Industrial Development Corporation on the said **‘Selected Agency’**, we _____

[Hereinafter referred to as ‘**the Bank**’ which expression shall include its successors and assigns]

do hereby undertake to pay **Maharashtra Industrial Development Corporation** an amount not exceeding Rs. _____ [Rupees_____] on demand made by **Maharashtra Industrial Development Corporation** on us due to a breach committed by the said **‘‘Selected Agency’’** of the terms and conditions of the **Order**.

1. We _____ **the Bank** hereby undertake to pay the amount under the guarantee without any demur merely on a demand received in writing from **Maharashtra Industrial Development Corporation** stating that the **‘‘Selected Agency’’** has committed breach of the term(s) and/or condition(s) contained in the **Order** and/or failed to comply with the terms and conditions as stipulated in the **Order** or amendment(s) thereto. The demand made on **the Bank** by **Maharashtra Industrial Development Corporation** shall be conclusive as to the breach of the term(s) and/or

condition(s) of the **Order** and the amount due and payable by **the Bank** under this guarantee, notwithstanding any dispute or disputes raised by the said **''Selected Agency''** regarding the validity of such breach and we agree to pay the amount so demanded by **Maharashtra Industrial Development Corporation** forthwith and without any demur. However, our liability under this guarantee shall be restricted to an amount not exceeding Rs. _____ [Rupees _____].

2. We, _____ the Bank further agree that this irrevocable guarantee herein contained shall remain in full force and effect during the period that would be taken for the performance of the said Order and that it shall continue to be enforceable till all the dues of Maharashtra Industrial Development Corporation under or by virtue of the said Order have been fully paid and its claim satisfied or discharged or till Maharashtra Industrial Development Corporation certifies that the terms and conditions of the Order have been fully and properly carried out by the ''Selected Agency'' and accordingly discharge the guarantee.
3. We _____ the Bank, undertake to pay to Maharashtra Industrial Development Corporation any money so demanded not withstanding any dispute or disputes raised by the said ''Selected Agency'' in any suit or proceedings pending before any court or tribunal relating thereto as our liability under this present being absolute and unequivocal. The payment so made by us under this Guarantee shall be valid discharge of our liability for payment there under and they said ''Selected Agency'' shall have no claim against us for making such payment.
4. We _____ the Bank further agree that Maharashtra Industrial Development Corporation shall have full liberty, without our consent and without affecting in any manner our obligation hereunder to vary any of the terms and conditions of the Order or to extend time of performance by the said ''Selected Agency'' from time to time or to postpone, for any time or from time to time, any of the powers exercisable by the Maharashtra Industrial Development against the said ''Selected Agency'' and to forbear or enforce any of the terms and conditions relating to the Order and shall not be relieved from our liability by reason of any such variation or extension being granted to the said ''Selected Agency'' or for any forbearance, act or omission on the part of Maharashtra Industrial Development Corporation or any indulgence by MIDC to the 'Selected Agency' or by any such matter or thing whatsoever which under the law relating to sureties would but for this provisions have effect of so relieving us.
5. In order to give full effect to this guarantee, Maharashtra Industrial Development Corporation will be entitled to act as if the BANK were the principal debtor and the BANK hereby waives all rights of surety ship.
6. Our liability under this bank guarantee is restricted to Rs._____ [Rupees_____] and shall remain in force up to _____ and thereafter till the expiry of the extended period, if any, (hereinafter Validity period) (the period should be additional six months from effective period of security/performance guarantee) Unless a demand is made under this guarantee

on us in writing at any time from the date of issue of the guarantee till the expiry of the Validity period including additional period of six months over contractual/extended period, we shall be discharged from all liabilities under this guarantee thereafter.

7. The claim, if any, under this guarantee, shall be lodged at (address of BANK & Branch) _____.
8. This guarantee will not be discharged due to change in the constitution in the Bank or the said ‘‘Selected Agency’’ or the provision of the contract between ‘‘Selected Agency’’ and Maharashtra Industrial Development Corporation.
9. The BANK hereby agrees that the Courts in Mumbai shall have exclusive jurisdiction in any matter of dispute between Maharashtra Industrial Development Corporation (MIDC) and the Bank and the Bank hereby agrees to address all the future correspondence in regard to this bank guarantee to Maharashtra Industrial Development Corporation at its registered office in MIDC Udyog Sarathi, Mahakali Caves Road, Mumbai, INDIA.
10. We have the power to issue this Guarantee in your favour under the Charter of our Bank and the undersigned has full power to execute this Guarantee under the Power of Attorney granted to him by the Bank.
11. We, _____ the Bank lastly undertake not to revoke this guarantee during its currency except with the previous consent of the Maharashtra Industrial Development Corporation (MIDC) in writing.
12. SIGNED AND DELIVERED ON THIS _____ DAY OF _____

Yours faithfully,

Signature of Authorized Official of bank

Name of the Official :

Designation of the Official :

Name of Bank :

Branch :

Address of Branch :

Telephone / Mobile No :

Email Id :

Annexure XIV – Manufacturer's Authorization Form (MAF)

To,

The General Manager,
IT Cell, MIDC Udyog Sarathi,
Mahakali Caves Road,
Mumbai-400093

Subject: Request for Proposal (RFP) for 'Selection of Agency for Implementing Cloud-based Enterprise Email Solution with Email Security, Data Protection and Backup Services for MIDC'.

Ref : Tender No: XXXXXXXXX Dated: XX/XX/XXXX

Dear Sir / Madam,

We, [Company Name], hereby authorize [Bidder's Name] to submit a bid, negotiate, and conclude the contract with [Purchaser/Organization Name] for Selection of Agency for Implementing Cloud-based Enterprise Email Solution with Email Security, Data Protection and Backup Services for MIDC as specified in the Request for Proposal (RFP) / Tender Document.

We hereby confirm that:

- **[Bidder's Name]** is duly authorized to represent and act on behalf of **[Company Name]** in all matters related to the Selection of Agency for Implementing Cloud-Based Email Solution for Maharashtra Industrial Development Corporation (MIDC).
- **[Company Name]**, in coordination with the Original Equipment Manufacturer (OEM) - shall provide all necessary technical support, services, warranty, and maintenance as per the terms and conditions of the contract entered into with MIDC.
- All products and services offered under this engagement fully comply with the specifications, standards, and requirements detailed in the MIDC RFP document.

This authorization shall remain valid until the successful completion of all contractual obligations associated with the project.

Yours faithfully,

For and on behalf of M/s _____ (Name of the Company)

Signature:

Name	:	
Designation	:	**Company Seal**
Address	:	
Telephone & Fax	:	
E-mail address	:	
Date	:	

Note: *This letter of authority should be on the letterhead of the concerned OEM and should be Ink signed by an authorized signatory of the OEM.*

Annexure XV – Data Security Declaration

To,

The General Manager,

IT Cell, MIDC Udyog Sarathi,

Mahakali Caves Road,

Mumbai-400093

Subject – Data Security Certificate in response to RFP for Implementation of Cloud-based Enterprise Email Solution with Email Security, Data Protection and Backup Services for MIDC.

Reference: Tender bearing no. <Tender no.> published on <Publication Date>

I / We hereby certify that the Office of MIDC (Maharashtra Industrial development Corporation) shall have absolute right on the digital data and output products processed / produced by me / us. I / We shall be responsible for security / safe custody of data during processing. I / We also certify that the digital topographical data will not be taken out of the MIDC network on any media by any means by me/us or any other person deployed by me/us. The original input data supplied to me / us by the Office of MIDC (Maharashtra Industrial development Corporation) or digital data and output products processed / produced from input data will not be passed on to any other agency or individual other than the authorized person of MIDC. I / We shall abide by all security and general instructions issued by MIDC or a person authorized by MIDC from time to time.

I / We also agree that any data pertaining to MIDC will be handed over / removed (as the case maybe) from my / our possession in the presence of person(s) authorized by MIDC after completion of the task.

Yours Sincerely,

_____

Signature of Proposed Resources & Counter Signed by Authorized Signatory (with official seal)

Name	:
Designation	:
Address	:
Telephone & Fax	:
E-mail address	:
Date	: