GUJARAT INFORMATICS LIMITED
(A Government of Gujarat Company)

GUJARAT INFORMATICS LIMITED
Block No. 2, 2nd Floor, Karmayogi Bhavan,
Sector-10A, Gandhinagar 382 010

Request for Proposal (RFP) for Red Team Exercise at Gujarat Security Operations Center (GSOC).

DISCLAIMER

GIL through this RFP invites proposals from reputed firms (hereafter referred as 'Bidders') which meets the evaluation criteria and can get onboarded to offer Red Team Exercise to various Government Departments / Boards / Corporations.

The information contained in this Request for Proposal (RFP) document or subsequently provided to Bidder(s), whether verbally or in documentary or any other form by or on behalf of the Gujarat Informatics Limited (GIL)/DST, Government of Gujarat or any of their employees or consultants, is provided to Bidder(s) on the terms and conditions set out in this RFP and such other terms and conditions subject to which such information is provided.

The purpose of this RFP is to provide interested parties with information that may be useful to them in eliciting their financial offers (the "Proposal") pursuant to this RFP. This RFP includes statements, which reflect various assumptions and assessments arrived at by the TENDERER, in relation to the RFP. Such assumptions, assessments and statements do not purport to contain all the information that each Bidder may require. This RFP may not be appropriate for all persons, and it is not possible for the TENDERER, its employees, or Consultants to consider the investment objectives, financial situation and particular need of each party who reads or uses this RFP. The assumptions, assessments, statements, and information contained in this RFP, may not be complete, accurate, adequate, or correct. Each Bidder should, therefore, conduct its own surveys and analysis and should check the accuracy, adequacy, correctness, reliability and completeness of the assumptions, assessments, statements, and information contained in this RFP and obtain independent advice from appropriate sources before filling up the RFP. Any deviation in the specification or proposed solutions will be deemed as incapability of the respective Agency and shall not be considered for final evaluation process.

Information provided in this document to the Bidder(s) is on a wide range of matters, some of which depends upon interpretation of law. The information given is not an exhaustive account of statutory requirements and should not be regarded as a complete or authoritative statement of law. The TENDERER accepts no responsibility for the accuracy or otherwise for any interpretation or opinion on law expressed herein.

TENDERER- its employees and advisors make no representation or warranty and shall have no liability to any person, including any Applicant or Bidder under any law, statute, rules or regulations or tort, principles of restitution or unjust enrichment or otherwise for any loss, damages, cost or expense which may arise from or be incurred or suffered on account of anything contained in this RFP or otherwise, including the accuracy, adequacy, correctness, completeness, delay or reliability of the RFP and any assessment, assumption, statement or information contained therein or deemed to form part of this RFP or arising in any way during the Bidding process.

Definitions

Authorized Signatory	The bidder's representative (explicitly, implicitly, or through conduct) with the powers to commit the authorizing organization to a binding agreement.
Bid	"Bid" means the response to this document presented in Single Packet, Technical Cum Commercial Bid and Financial Bid, which are supplied with necessary documents and forms as given in Annexure, complete in all respect adhering to the instructions and spirit of this document.
Bidder	"Bidder" means any individual/proprietor/ partnership firm/ agency/ company/ responding to Request for Proposal and who submits Bid.
Contract	Means the contract of service entered between the User Department and the "Service Provider" for Red Team Exercise at Gujarat Security Operations Center (GSOC) with the entire documentation specified in the RFP.
Day	"Day" means a working day as per rules of User Department.
EMD	Earnest Money Deposit
DD	Demand Draft
Purchaser	User Department
TC	Tender Committee
PBG	Performance Bank Guarantee
Security Deposit (SD)	Amount of the Order Value deposited by the Bidder and retained till the successful completion of the project (as long as the bidder fulfils the contractual agreement).
RFP	"RFP" means the Request for Proposal
Work Order	"Work Order" shall mean the Purchase Order/Work order and its attachments and exhibits issued by User Department
Consignee	"Consignee" shall mean User Department.
Client	User Department/User Department's Client
Validity of Documents	Validity of all the documents shall be counted from the last date of submission of bids

SECTION – 1

1. Purpose of this Document

This Request for Proposal (RFP) document has been prepared solely for the purpose of enabling GIL to select Service Provider for conducting Red Team Exercise to simulate a real-world attack on an DST/GOG's Projects (such as GSDC, SOC, GSWAN, GISL, GFGNL - IT infrastructure) to assess and improve its strength of defense.

The GIL, for this purpose, invites proposal from Bidders who are interested in participating in this RFP who fulfill the eligibility criteria mentioned in this RFP and are also in a position to comply with the technical requirement as mentioned in RFP. Apart from the above the bidder must also agree to all our terms & conditions mentioned under this RFP.

The RFP document is not recommendation, offer or invitation to enter into a contract, agreement or any other arrangement, in respect of the services. The provision of the services is subject to observance of selection process and appropriate documentation being agreed between the GIL and any successful Bidder as identified by the GIL, after completion of the selection process as detailed in this document.

GIL may, at its own discretion, extend the date for submission of bids. In such case, all rights and obligations of the GIL and bidders previously subject to the deadline will thereafter be subject to the deadline as extended.

1.1 Information Regarding RFP

Proposal in the form of BID is requested for the item(s) in complete accordance with the documents/attachments as per following guidelines.

i. Bidder shall upload their bids on https://gem.gov.in/
ii. Bids complete in all respects should be uploaded on or before the BID DUE DATE.
iii. In the event of the date specified for receipt and opening of bid being declared as a holiday for GIL office, the due date for submission of bids and opening of bids will be the next working day at the appointed time.
iv. Services offered should be strictly as per requirements mentioned in this Bid document.
v. Please spell out any unavoidable deviations, Clause/ Article-wise in your bid under the heading Deviations.
vi. Once quoted, the bidder shall not make any subsequent price changes, whether resulting or arising out of any technical / commercial clarifications sought regarding the bid, even if any deviation or exclusion may be specifically stated in the bid. Such price changes shall render the bid liable for rejection.
vii. The bid submitted should be valid for a period of 180 days from the date of bid opening.

1.2 Instruction to the bidders for online bid submission

i. Tender documents are available only in electronic format which Bidders can download free of cost from the website https://gil.gujarat.gov.in and https://gem.gov.in/.
ii. The bids have been invited through GeM portal, i.e. the eligibility criteria, technical and financial stages shall be submitted online on the GeM portal https://gem.gov.in/.
iii. Interested and eligible Bidders are required to upload the eligibility related document in eligibility bid section, Technical related document in Technical bid section & Commercial Bid in Commercial bid section. The Technical & Commercial Bid must be uploaded to https://gem.gov.in/.
iv. In case of any clarifications required, please contact Deputy General Manager (Technical), GIL in writing 2 days before the Pre-Bid meeting date.
v. In case the bidders need any support related to bidding on https://gem.gov.in , Bidder may also send their clarifications on dgmtech-gil@gujarat.gov.in and mgrhninfra1-gil@gujarat.gov.in . also, bidder may contact the following office:

DGM (Tech)

Gujarat informatics ltd

Block No. 2, 2nd floor, Karmayogi bhavan, Gandhinagar-382010

1.3 Fact Sheet

1.	GIL Contact person	**Deputy General Manager (Technical)** **E-mail:** dgmtech-gil@gujarat.gov.in, mgrhninfra1-gil@gujarat.gov.in **Contact-079-232-52026/59227**

Note:

1) The TENDERER reserves all the rights to cancel the process and reject any or all the proposals at any time.
2) No contractual obligation whatsoever does arise from the RFP document/process unless and until a formal contract is signed and executed between the TENDERER and the successful proposers.
3) The TENDERER disclaims any factual or other errors in the RFP document (the onus is purely on the individual proposers to verify such information) and the information provided therein are intended only to help the proposers to prepare a logical proposal.

SECTION 2: ELIGIBILITY CRITERIA

Evaluation will be based on the firm meeting the Pre- qualification criteria. It is mandatory for the firm (as an individual or in consortium) to fulfill all the pre-qualification criteria to be technically qualified. The DST/GIL reserves the right to assess the firm's capability and capacity in the overall interest of the project.

2.1 PQ Criteria for bidders

Sr.no	Basic Requirement	Specific Requirement	Documents Required
1.	Legal Entity	Bidder should be an Indian firm • Bidder should be registered under the Companies Act 1956 or 2013 in India or a Proprietorship or partnership or an agency should be a firm/LLP at the time of the bidding • Bidder should have a registered number of, GST, Income Tax / Pan number • Bidder should be in operation in India for a period of at least 5 years as on publication of this RFP.	a) Copy of certification of incorporation issued by competent authority / registration Certificate/ Shop& Establishment certificate b) Copy of PAN card c) Copy of GST registration
2.		Bidder must have a Government Organization / PSU / PSE / partnership firm / LLP or private / public limited company in India at least for the last 5 years.	a) Certificate Of Incorporation b) Memorandum and Article of Association
3.	CERT-In Empaneled	Bidder should be a CERT-IN Empaneled	Active Cert-In Empanelment Proof
4.	Financial Turnover	The Bidder must have average turnover of Rs. 80 Lacs or more in the last three financial years. (FY 21-22, FY22-23, FY 23-24).	CA certified and audited Balance Sheet and Profit & Loss statement for any three of last four audited financial years (2020-21, (FY 21-22, FY22-23, FY 23-24). CA certificate mentioning turnover and Net worth from the said business.
5.	Financial Net worth	The Bidder must have Net profit-making entity continuously for the last three years	Audited Financials/CA certificate
6.	Certification	The Bidder must have valid Certificate as on date of Bid submission. — ISO 9001:2015, — ISO 27001:2013, — SOC 2 TYPE 1 and 2 certified.	Valid Copy of certification
7.	Similar Experience	Bidder must have experience of carrying at least 3 Red team contract with any Central Government / State Government / /BFSI/PSU's /PSB's. in last 5 years in India.	— Copy of the Work order/Purchase Order — Certificate of completion of the work from client — Project Citation with Client details (Name, Designation, Contact Number, Email Id, etc.)
8.		The Bidder shall provide reference of at least three clients in India where respondent must be doing Red team	Name: Contact Person:

		contract. Include short descriptions, dates, and client references (client contact person, address, and phone number) in the proposal	Contact Number Email id: Services Offered:
9.	Resources	The Bidder should have at least 6 qualified resources on their own company payroll with below certification and experience: — Minimum 2 Qualified resources from CISA / CISSP /CISM /OSCE Certification and — Minimum 2 Qualified resources from OSCP / CRTA / ECPPT professional Certification and — Min 2 CEH professional certification Project Manager should have minimum 5 years' of experience in Red team projects.	— Undertaking on company letter head duly signed by the authorized signatory of the company confirming on the Name or resources, Year of relevant experience and Certifications. — The Bidder should also submit the profile of proposed minimum 2 (two) resources who will be deployed under this assignment.
10.	Blacklisting	Bidder must not be blacklisted / debarred by any Statutory, Regulatory or Government Authorities or Public Sector Undertakings (PSUs / PSBs).	Undertaking on a company letter lead dully signed by the authorized signatory of the company
11.	Local Office	The bidder should have local office in Gujarat or should submit a declaration for establishing an office in Gujarat within 30 days of issuing of PO from tenderer.	Registration Certificate / Sale Deed / Rental Agreement/ Utility Bill in the name of the company or Declaration that the office will be set-up in Gujarat within a period of 30 days from the date of issuance of Letter of Intent.

Note:

1. All the details and the supportive documents for the above-mentioned items should be uploaded in the bid.
2. Bidder's experience, bidder's turn over criteria will not be considered of GeM bid, however bidder must match eligibility criteria, experience, bidder's turn over criteria, as mentioned in this document and will be considered for evaluation.
3. Existing GSDC team, GSOC team and TPA team are not allowed to participate in this BID. In addition, any team involved at GSDC for security related activities may not be able to participate.

2.2 Technical Evaluation

Bidders who meet the pre-qualifications/eligibility requirements as on date of bid submission would be considered as qualified to move to the next stage of technical evaluations. Based on technical evaluation framework mentioned, the Committee shall evaluate each proposal and allot technical score as per the Technical Criteria mentioned below.

Evaluation Criteria	**Parameters**	**Max Marks**	**Remarks**
Past Project Experience	Bidder to have experience of at Red Team Projects in last 5 years.	**20**	— Copy of the Work order/Purchase Order

	3 Projects – 10 Marks 4 Projects – 15 Marks 5 Projects – 20 Marks		— Certificate of completion of the work from client — Project Citation with Client details (Name, Designation, Contact Number, Email Id, etc.)
Past Project References	Bidder to provide 3 customer references in India. 3 Customer Reference = 6 Marks 4 Customer Reference = 13 Marks 5 Customer Reference = 20 Marks	**20**	— Copy of the Work order/Purchase Order — Certificate of completion of the work from client — Project Citation with Client details (Name, Designation, Contact Number, Email Id, etc.)
Number of Qualified resources on bidder's Payroll	Qualified Resources with Certifications: - Qualified resources with CISA /CISSP /CISM /OSCE certification – 1 Marks each, **Maximum up to 5 Marks** - Qualified resources with OSCP /CRTA /ECPPT professional certification – 1 Marks each, **Maximum up to 4 Marks** - Qualified resources with CEH professional certification – 0.5 Marks each, Maximum up to **1 Marks**	**10**	The Bidder should also submit the profile of each resource with their respective certificates.
Methodology & Approach	Bidder approach for executing the Project. It should cover Bidder's understanding on scope and methodology to be adopted for delivering the program deliverables. It should also cover bidder's experience & citations.	**30**	Presentation to be given by bidder on approach and methodology. Technical Proposal that shall be a part of the submitted bid shall be presented.
Reporting	Bidder to share the sample report with all the parameters and components that shall be incorporated in the final assessment report as the scope of the bid.	**20**	Marks to be allocated on basis of Quality/Parameters/Detail oriented in the sample report submitted.
Total		**100**	

Note:

i. Technical evaluation shall include the evaluation of all the documents mentioned in the Technical Bid.

ii. The bidder shall be required to get at least 70% marks to qualify for next stage i.e. opening of the financial bids.

2.3 Overall Evaluation (Lowest Bid Value)

i. Bid evaluation committee will evaluate and compare the bids determined to be substantially responsive. It is bid evaluation committee's intent to select the proposal that is most responsive to the project needs and each proposal will be evaluated using the criteria and process outlined in this section.

ii. The evaluation shall be strictly based on the information and supporting documents provided by the bidders. It is the responsibility of the bidders to provide all supporting documents as listed in forms necessary to fulfill the mandatory eligibility criteria.

iii. Technical bids shall be examined by the bid evaluation committee with respect to compliance,

completeness and suitability of the proposal to the project and only the bids which are complying to the requirements mentioned in the RFP shall be considered as technically qualified.

iv. Pre-Qualification and the Technical criteria of all the Bidders will be evaluated for financial bid opening.

v. Only the bidders, who score a technical bid score (Tb) of 70 (Seventy) or more, will qualify for the financial bid evaluation.

vi. Total bid evaluation: Only the financial bids of those bidders qualified in the technical evaluation shall be opened and the decision of GIL in this regard shall be final; financial bids of the other bidders will not be accepted.

vii. Shortlisted bidder quoting lowest bid value will be considered for final selection as L1.

viii. If the L1 Bidder is not agreed to execute the project for any reason, Tenderer may call L2 Bidder to match the price of L1. If L2 bidder agree to match the price of L1, tenderer may award the contract to L2 bidder to execute the Project. The same process may be followed for remaining qualified Bidders.

Note:

1. Financial Bids that are not as per the format provided in the RFP shall be liable for rejection.

2. The Bidder must attach valid documents in support to their Technical and Financial capabilities /strength, as mentioned above. Without proper supporting documents, the Bid proposals are liable for rejection.

SECTION 3: INSTRUCTIONS TO BIDDERS

3.1 General Instruction to Bidders

All information supplied by Bidders may be treated as contractually binding on the Bidders on successful award of the assignment by the TENDERER based on this RFP. No commitment of any kind, contractual or otherwise shall exist unless and until a formal written contract has been executed by or on behalf of the TENDERER. Any notification of preferred bidder status by the TENDERER shall not give rise to any enforceable rights by the Bidder. The TENDERER may cancel this public procurement at any time prior to a formal written contract being executed by or on behalf of the TENDERER.

This RFP supersedes and replaces any previous public documentation, communications, and Bidders should place no reliance on such communications. The TENDERER may terminate the RFP process at any time and without assigning any reason. The TENDERER makes no commitments, express or implied, that this process will result in a business transaction with anyone.

3.2 Cost of Bidding

3.2.1 The Bidder shall bear all costs associated with the preparation and submission of the Bid. The TENDERER will in no case be responsible for those costs, regardless of the conduct or outcome of the bidding process.

3.2.2 Bidder is requested to EMD in cover to GIL. In case of non-receipt of physical EMD the bid will be rejected by GIL/Dept. of Science & Technology as non-responsive.

3.3 Amendment of Bidding Documents

At any time prior to the deadline for submission of bids, the TENDERER, for any reason, whether at its own initiative or in response to the clarifications requested by prospective bidders may modify the bidding documents by amendment & put on our websites.

All prospective bidders are requested to browse TENDERER'S website & any amendments/ corrigendum/modification will be notified on the website and such modification will be binding on them. To allow prospective bidders a reasonable time to take the amendment into account in preparing their bids, the TENDERER, at its discretion, may extend the deadline for the submission of bids.

3.4 Language of Bid

3.4.1 The Bid prepared by the Bidder, as well as all correspondence and documents relating to the Bid exchanged by the Bidder and the TENDERER shall be in English.

3.5 Bid Security/ Earnest Money Deposit (EMD)

3.5.1 Bidders shall submit EMD of in the form of a Demand Draft OR in the form of an unconditional Bank Guarantee by Bank Guarantee (which should be valid for 6 months from the last date of bid submission) of any Nationalized Bank including the public sector bank or Private Sector Banks or Commercial Banks or Co-Operative Banks and Rural Banks (operating in India having branch at Ahmedabad/Gandhinagar) as per the G.R. no. FD/MSM/e-file/4/2023/4020/D.M.O. dated 11.03.2024 issued by Finance Department or further instruction issued by Finance department time to time; in the name of "Gujarat Informatics Ltd." payable at Gandhinagar .

OR

Bidders can also submit the EMD with Payment Online through RTGS/internet banking in Beneficiary name Gujarat Informatics Ltd., Account No. 50200010918090, IFSC Code HDFC0000190, Bank Name HDFC Bank Ltd. Branch address Sector-16, Gandhinagar Branch.

3.5.2 EMD of all unsuccessful bidders would be refunded by GIL within 60 Days on selection of successful bidder.

3.5.3 The EMD of the successful bidder would be returned upon successful submission of Performance Bank Guarantee as per the format provided in Format IV.

3.5.4 EMD amount is interest free and will be refundable to the unsuccessful bidders without any accrued interest on it.

3.5.5 The bid / proposal submitted without EMD and Bid Processing fee, mentioned above, will be summarily rejected.

3.5.6 The EMD may be forfeited, In case of a Bidder if:

3.5.6.1 The bidder withdraws its bid during the period of bid validity.

3.5.6.2 The Bidder does not respond to requests for clarification of their Bid.

3.5.6.3 The Bidder fails to co-operate in the Bid evaluation process.

3.5.6.4 In case of successful bidder, the said bidder fails:

3.5.6.4.1 Fails to sign the agreement in time

3.5.6.4.2 Fails to submit performance bank guarantee

3.6 Late Bids

3.6.1 Bids received after the due date and the specified time (including the extended period if any) for any reason whatsoever, shall not be entertained and shall be REJECTED.

3.6.2 The bids submitted by telex/ telegram/ fax/ e-mail etc. shall not be considered. No correspondence will be entertained on this matter.

3.7 Section Comprising the Bids

3.7.1 All forms / Tables, duly filled-in with necessary proofs, as required and stated in the bid document & supporting documents for eligibility criteria should be uploaded. The bid uploaded shall have the following documents:

3.7.1.1 BID SECURITY SECTION:

The bid security & bid processing fee (non-refundable) to be furnished to GIL office in the form of demand draft in favour of "Gujarat Informatics Ltd." payable at Ahmedabad/Gandhinagar before the last date and time of the bid submission.

3.7.1.2 ELIGIBILITY SECTION

1.) Financial Details of the Bidder. (In the Prescribed Format)

2.) Bidder's Experience. (In the Prescribed Format)

3.7.1.3 **PRICE BID SECTION**

Priced bid (in the prescribed format only as given in this RFP)

Note: Filling up prices anywhere other than the prescribed shall render the bidder disqualified.

3.7.1.4 Annexures & Formats

3.7.1.4.1 Wherever a specific form is prescribed in the Bid document, the Bidder shall use the form to provide relevant information. If the form does not provide space for any required information, space at the end of the form or additional sheets shall be used to convey the said information. Failing to submit the information in the prescribed format, the bid is liable for rejection.

3.7.1.4.2 For all other cases, the Bidder shall design a form to hold the required information.

3.7.1.4.3 TENDERER shall not be bound by any printed conditions or provisions in the Bidder's Bid Forms

3.7.2 The prices shall strictly be submitted in the given format. Quoted prices shall be without GST. The tax (GST) components as applicable shall be mentioned separately. Successful Bidder will have to supply/provide Services with an Invoice from a place located within State of Gujarat.

3.7.3 Prices shall be written in both words and figures. In the event of difference, the price in words shall be valid and binding. Arithmetical errors will be rectified on the following basis.

3.7.4 Offered price should be exclusive of all applicable taxes (anywhere in Gujarat state).

3.8 Bid Opening

3.8.1 Bids will be opened in the presence of Bidder's representatives, who choose to attend. The Bidder's representatives who are present shall sign a register evidencing their attendance.

3.8.2 In the event of the specified date of Bid opening being declared a holiday for the GIL, the Bids shall be opened at the appointed time and location on the next working day.

3.8.3 The Bidder's names, bid modifications or withdrawals, discounts and the presence or absence of relevant Bid security and such other details as the TENDERER officer at his/her discretion, may consider appropriate, will be announced at the opening.

3.8.4 Immediately after the closing time, the TENDERER contact person shall open the Un-Priced Bids and list them for further evaluation.

3.8.5 Bids that are not opened at bid opening shall not be considered further for evaluation.

3.9 Bid Validity

3.9.1 Bids shall remain valid for 180 days after the date of Bid opening prescribed by the TENDERER. A Bid valid for a shorter period shall be rejected as non-responsive.

3.9.2 In exceptional circumstances, the TENDERER may solicit Bidder's consent to an extension of the period of validity. The request and the responses thereto shall be made in writing. The Bid security shall also be suitably extended. A Bidder's request to modify the Bid will not be permitted.

3.10 Contacting the Tenderer

Bidder shall not approach the TENDERER officers outside of office hours and/ or outside the TENDERER office Premises, from the time of the Bid opening to the time the Contract is awarded. Any effort by a bidder to influence the TENDERER officers in the decisions on Bid evaluation, bid comparison or contract

award may result in rejection of the Bidder's offer. If the Bidder wishes to bring additional information to the notice of the TENDERER, it should do so in writing.

3.11 Rejection of Bids

The TENDERER reserves the right to reject any Bid, and to annul the bidding process and reject all bids at any time prior to award of Contract, without thereby incurring any liability to the affected Bidder(s) or any obligation to inform the affected Bidder(s) of the grounds for such decision.

3.12 Bid Evaluation Process

3.12.1 The TENDERER will form a Committee which will evaluate the proposals submitted by the bidders for a detailed scrutiny. During evaluation of proposals, the TENDERER, may, at its discretion, ask the bidders for clarification of their Proposals.

3.12.2 The bidders are expected to provide all the required supporting documents & compliances as mentioned in this RFP.

3.12.3 During the evaluation, committee may seek the clarification in writing from the bidder, if required. If bidder fails to submit the required clarifications in due time, the evaluation will be done based on the information submitted in the bid.

3.13 Notification of Award & Signing of Contract

3.13.1 Prior to expiration of the period of Bid validity, the TENDERER will notify the successful Bidders and issue LoI.

3.13.2 Within fifteen (15) calendar days of receipt of the Contract Form, the successful Bidder shall sign the Contract and return it to the TENDERER.

3.14 Force Majeure

Force Majeure shall mean any event or circumstances or combination of events or circumstances that materially and adversely affects, prevents or delays any Party in performance of its obligation in accordance with the terms of the Agreement, but only if and to the extent that such events and circumstances are not within the affected party's reasonable control, directly or indirectly, and effects of which could have prevented through Good Industry Practice or, in the case if construction activities through reasonable skill and care, including through the expenditure of reasonable sums of money. Any events or circumstances meeting the description of the Force Majeure which have same effect upon the performance of any contractor shall constitute Force Majeure with respect to the bidder. The Parties shall ensure compliance of the terms of the Agreement unless affected by the Force Majeure Events. The bidder shall not be liable for forfeiture of its implementation / Performance guarantee, levy of Penalties, or termination for default if and to the extent that it’s delays in performance or other failure to perform its obligations under the Agreement is the result of Force Majeure.

3.14.1 Force Majeure Events

The Force Majeure circumstances and events shall include the following events to the extent that such events or their consequences (it being understood that if a causing event is within the reasonable control of the affected party, the direct consequences shall also be deemed to be within such party's reasonable control) satisfy the definition as stated above. Without limitation to the generality of the foregoing, Force Majeure Event shall include following events and circumstances and their effects to the extent that they, or their effects, satisfy the above requirements:

3.14.2 **Natural events** (“Natural Events”) to the extent they satisfy the foregoing requirements including:

- 3.14.2.1 Any material effect on the natural elements, including lightning, fire, earthquake, cyclone, flood, storm, tornado, or typhoon;
- 3.14.2.2 Explosion or chemical contamination (other than resulting from an act of war);
- 3.14.2.3 Epidemic such as plague;
- 3.14.2.4 Any event or circumstance of a nature analogous to any of the foregoing.

3.14.3 Other Events (“Political Events”) to the extent that they satisfy the foregoing requirements including:

3.14.3.1 Political Events which occur inside or Outside the State of Gujarat or directly involve the State Government and the Central Government ("Direct Political Event"), including:

- Act of war (whether declared or undeclared), invasion, armed conflict or act of foreign enemy, blockade, embargo, revolution, riot, insurrection, civil commotion, act of terrorism or sabotage;
- Strikes, work to rules, go-slows which are either widespread, nation- wide, or state-wide or are of political nature;
- Any event or circumstance of a nature analogous to any of the foregoing.

3.14.4 **FORCE MAJEURE EXCLUSIONS:**

Force Majeure shall not include the following event(s) and/or circumstances, except to the extent that they are consequences of an event of Force Majeure:

3.14.4.1 Unavailability, late delivery

3.14.4.2 Delay in the performance of any contractor, sub-contractors, or their agents;

3.14.5 **PROCEDURE FOR CALLING FORCE MAJEURE**:

The Affected Party shall notify to the other Party in writing of the occurrence of the Force Majeure as soon as reasonably practicable, and in any event within 05 (five) days after the Affected Party came to know or ought reasonably to have known, of its occurrence and that the Force Majeure would be likely to have a material impact on the performance of its obligations under the Agreement.

3.15 Contract Obligations

Once a contract is confirmed and signed, the terms and conditions contained therein shall take precedence over the Bidder's bid and all previous correspondence.

3.16 Amendment to the Agreement

Amendments to the Agreement may be made by mutual agreement by both the Parties. No variation in or modification in the terms of the Agreement shall be made except by written amendment Signed by both the parties. All alterations and changes in the Agreement will consider prevailing rules, regulations, and laws applicable in the state of Gujarat.

3.17 Representations and Warranties

3.17.1 Representations and Warranties by the Selected Agency**:**

3.17.1.1 It is a company duly organized and validly existing under the laws of India and has all requisite legal power and authority and corporate authorizations to execute the Agreement and carry out the terms, conditions, and provisions hereof. It has in full force and effect all requisite clearances, approvals and permits necessary to enter into the Agreement and perform its obligations hereof.

3.17.1.2 The Agreement and the transactions and obligations hereof do not contravene its constitutional documents or any law, regulation or government directive and will not contravene any provisions of, or constitute a default under, any other Agreement or instrument to which it is a party or by which it or its property may be bound or any of its obligations or undertakings by which it or any of its assets are bound or cause a limitation on its powers or cause it to exceed its authorized powers.

3.17.1.3 There is no pending or threatened actions, suits or proceedings affecting the Successful Bidder or its affiliates or any of their respective assets before a court, governmental agency, commission or arbitrator or administrative tribunal which affects the Successful Bidder's ability to perform its obligations under the Agreement; and neither Successful Bidder nor any of its affiliates have immunity from the jurisdiction of a court or from legal process (whether through service of notice, attachment prior to judgment, attachment in aid of execution or otherwise). The Successful Bidder confirms that all representations and warranties of the bidder set forth in the Agreement are true, complete, and correct in all respects.

3.17.1.4 No information given by the Successful Bidder in relation to the Agreement, project documents or any document comprising security contains any material wrong statement of fact or omits to state as fact which would be materially averse to the enforcement of the rights and remedies of TENDERER or which would be necessary to make any statement, representation or warranty contained herein or therein true and correct.

3.17.2 Representations and Warranties by the TENDERER

3.17.2.1 It has full legal right; power and authority to execute the said project and to enter and perform its obligations under the Agreement and there are no proceedings pending.

3.17.2.2 The Agreement has been duly authorized, executed and delivered by the TENDERER and constitutes valid, legal, and binding obligation of TENDERER.

3.17.2.3 The execution and delivery of the Agreement with the selected agency does not violate any statutory judgment, order, degree, regulation, right, obligation or rule of any court, government authority or arbitrator of competent jurisdiction applicable in relation to the TENDERER, its assets, or its administration.

3.18 **Resolution of Disputes**

3.18.1 If any dispute arises between the Parties hereto during the subsistence or thereafter, in connection with the validity, interpretation, implementation or alleged material breach of any provision of the Agreement or regarding a question, including the questions as to whether the termination of the Contract Agreement by one Party hereto has been legitimate, both Parties hereto shall endeavour to settle such dispute amicably. The attempt to bring about an amicable settlement is considered to have failed as soon as one of the Parties hereto, after reasonable attempts [which attempt shall continue for not less than 30 (thirty) days], give 15 days' notice thereof to the other Party in writing.

3.18.2 In the case of such failure the dispute shall be referred to a sole arbitrator or in case of disagreement as to the appointment of the sole arbitrator to three arbitrators, two of whom will be appointed by each Party and the third appointed by the two arbitrators.

3.18.3 The place of the arbitration shall be Gandhinagar, Gujarat.

3.18.4 The Arbitration proceeding shall be governed by the Arbitration and Conciliation Act of 1996 as amended.

3.18.5 The proceedings of arbitration shall be in English language.

3.18.6 The arbitrator's award shall be substantiated in writing. The arbitration tribunal shall also decide on the costs of the arbitration procedure.

3.18.7 The Parties hereto shall submit to the arbitrator's award and the award shall be enforceable in any competent court of law.

3.19 Books & Records

The selected agency shall maintain adequate Documents Related to project's materials & equipment's for inspection and audit by the TENDERER during the terms of Contract until expiry of the performance guarantee.

3.20 Performance Guarantee

3.20.1 The Successful bidder has to submit Performance Bank Guarantee @ 10% of total order value within 15 days from the receipt of notification of award/Contract Signing for the duration of warranty of all Nationalized Bank including the public sector bank or Private Sector Banks authorized by RBI or Commercial Bank or Regional Rural Banks of Gujarat or Co-Operative Bank of Gujarat (operating in India having branch at Ahmedabad/Gandhinagar) as per the G.R. no. FD/MSM/e-file/4/2023/4020/D.M.O. dated 11.03.2024 issued by Finance Department or further instruction issued by Finance department time to time. (The draft of Performance Bank Guarantee is as per Section 8 of point no. 8.3(format-3).

3.20.2 The Performance Security shall be in the form of Bank Guarantee valid till 6 months from the date of contract expiry.

3.20.3 The proceeds of the performance security shall be payable to the GIL/DST as compensation for any loss resulting from the Service provider's failure to complete its obligations under the Contract.

3.20.4 The Performance Security will be discharged by GIL/DST and returned to the Bidder on completion of the bidder's performance obligations under the contract.

3.20.5 In the event of any contract amendment, the bidder shall, within 21 days of receipt of such amendment, furnish the amendment to the Performance Security, rendering the same valid for the duration of the Contract, as amended for further period.

3.20.6 No interest shall be payable on the Performance Bank Guarantee amount. GIL/DST may invoke the above bank guarantee for any kind of recoveries, in case; the recoveries from the bidder exceed the amount payable to the bidder.

3.21 Termination Clause

The TENDERER, reserves the right to suspend any of the services and/or terminate this agreement in the following circumstances by giving 30 days' notice in writing if: -

3.21.1 The bidder becomes the subject of bankruptcy, insolvency, and winding up, receivership proceedings;

3.21.2 In case the TENDERER finds illegal use of hardware, software tools, manpower etc. that are dedicated to the project;

3.21.3 If SLAs are not maintained properly and not provide services as per SLAs, then TENDERER has right to foreclose contract.

3.21.4 Upon occurrence of an event of default as set out in Clause above, either party will deliver a default notice in writing to the other party which shall specify the event of default and give the other party an opportunity to correct the default.

3.21.5 Upon expiry of notice period unless the party receiving the default notice remedied the default, the party giving the default notice may terminate the Agreement.

3.21.6 During the notice period, both parties shall, save as otherwise provided therein, continue to perform their respective obligations under this Agreement and shall not, whether by act of omission or commission impede or otherwise interfere with party's endeavour to remedy the default which gave rise to the commencement of such notice period.

3.21.7 The termination hereof shall not affect any accrued right or liability of either Party nor affect the operation of the provisions of the Contract that are expressly or by implication intended to come into or continue in force on or after such termination.

3.21.8 In case of termination bidder will be paid for the work/services already delivered till the date of termination after deduction of penalties, if any.

3.22 Indemnification

Selected agency will defend and/or settle any claims against the TENDERER that allege that Bidder service and/or branded product as supplied under this contract infringes the intellectual property rights of a third party. Selected agency will rely on Customer's prompt notification of the claim and cooperation with our defence. Bidder may modify the product or service to be non-infringing and materially equivalent or we may procure a license. If these options are not available, we will refund to Customer the amount paid for the affected product in the first year or the depreciated value thereafter or, for support services, the balance of any pre-paid amount

or, for professional services, the amount paid. Bidder is not responsible for claims resulting from any unauthorized use of the products or services. This section shall also apply to deliverables identified as such in the relevant Support Material except that Bidder is not responsible for claims resulting from deliverables content or design provided by Customer.

3.23 Limitation of Liability

Selected agency's cumulative liability for its obligations under the contract shall not exceed the value of the charges payable by the TENDERER within the remaining duration of the contract term from the day claim is raised.

3.24 Confidentiality

3.24.1 Selected agency understands and agrees that all materials and information marked and identified by the TENDERER as 'Confidential' are valuable assets of the TENDERER and are to be considered as proprietary information and property. Selected agency will treat all confidential materials and information provided by the TENDERER with the highest degree of care necessary to ensure that unauthorized disclosure does not occur. Selected agency will not use or disclose any materials or information provided by tenderer without its prior written permission.

3.24.2 Selected agency shall not be liable for disclosure or use of any materials or information provided by the TENDERER or developed by selected agency which is:

3.24.2.1 Possessed by selected agency prior to receipt from the TENDERER, other than through prior disclosure by the TENDERER, as documented by selected agency's written records;

3.24.2.2 Published or available to the public otherwise than through a breach of Confidentiality; or

3.24.2.3 Obtained by selected agency from a third party with a valid right to make such disclosure, provided that said third party is not under a confidentiality obligation to the TENDERER; or

3.24.2.4 Developed independently by the selected agency.

3.24.3 If selected agency is required by judicial or administrative process to disclose any information or materials required to be held confidential hereunder, selected agency shall promptly notify the TENDERER and allow reasonable time to oppose such process before making disclosure.

3.24.4 Selected agency understands and agrees that any use or dissemination of information in violation of this Confidentiality Clause will cause the TENDERER irreparable harm, may leave the TENDERER with no adequate remedy at law and the TENDERER is entitled to seek to injunctive relief.

3.24.5 The TENDERER does not follow the practice of asking Confidential Information of selected agency, however if any confidential information is required/shared by the selected agency then selected agency must clearly marked it as "Strictly confidential". The TENDERER in turn will not share the same without prior concern of the selected agency.

3.24.6 Above mentioned "confidentiality clause" shall be applicable on both the parties i.e., the TENDERER and the successful bidder.

3.25 Service Terms

3.25.1 The bidder shall provide and share regular reports used to monitor the Hosted environment.

3.25.2 The SLAs will be used to evaluate the performance of the services on Monthly basis.

3.25.3 Payment to the successful bidder will be impacted by the penalty levied for non-performance as per SLA requirements.

3.25.4 It is mandatory for Bidder to allocate a spokesperson and share the contact details with the department to facilitate them with day-to-day activity and helping them in maintaining the services.

3.25.5 The Bidder is responsible to maintain documentation on the progress of the work and will have to update the same on regular basis. Bidder will have to submit the progress reports regularly, as per the guidelines issued by TENDERER from time-to-time.

3.25.6 The bidder shall ensure that security measures, policies and procedures implemented are adequate to protect and maintain the confidentiality of the Confidential Information. Bidder also agrees and acknowledges that it shall adhere to reasonable security practices over all sensitive personal information of the said project as prescribed by various rules under I.T. Act, 2000 (as amended from time to time).

3.26 Fraudulent and Corrupt Practices

3.26.1 Fraudulent practice means a misrepresentation of facts to influence a procurement process or the execution of a Contract and includes collusive practice among Bidders (prior to or after Bid submission) designed to establish Bid prices at artificial non-competitive levels and to deprive the TENDERER of the benefits of free and open competition.

3.26.2 “Corrupt Practice” means the offering, giving, receiving, or soliciting of anything of value, pressurizing to influence the action of a public official in the process of Contract execution.

3.26.3 The TENDERER will reject a proposal for award and may forfeit the EMD and/or Performance Bank Guarantee if it determines that the bidder recommended for award has engaged in corrupt or fraudulent practices in competing for, or in executing, contract(s).

3.27 Non-Disclosure Agreement (NDA)

3.27.1 The agency shall sign a mutually agreed Non-Disclosure Agreement (NDA) with the TENDERER at the time of deployment. The format of NDA proposed to be signed shall be as per the Annexure. A copy of the signed NDA shall be provided to the agency by the TENDERER for record keeping / reference purpose.

3.27.2 The selected agency shall ensure that all its employees, agents and sub-contractors involved in the project, execute individual non-disclosure agreements, which have been duly approved by the Purchaser with respect to this Project. The implementing agency get NDAs signed from every resource involved in the project and submit it to purchaser. In case of replacement, the selected agency shall get the NDAs signed from new deployed resources and submit it to the purchaser.

3.28 Copyright and Intellectual Property Rights

3.28.1 The TENDERER shall be entitled to all intellectual property and other proprietary rights including, but not limited to, patents, copyrights, and trademarks, with regard to products, processes, inventions, ideas, know-how, or documents and other materials which the Bidder has developed for the performance of services under this RFP and which bear a direct relation to or are produced or prepared or collected in consequence of, or during the course of, the performance of services under this RFP, and the Bidder acknowledges and agrees that such products, documents and other materials constitute works made for hire for the TENDERER.

3.28.2 At the request of TENDERER, the Bidder shall take all necessary steps, execute all necessary documents and generally assist in securing all such proprietary rights and transferring or licensing them to the TENDERER in compliance with the requirements of the applicable law and this RFP.

3.28.3 All IPR in relation to project documents, assets, resources, designs, drawings, estimates, recommendations, source codes, etc. shall vest with the TENDERER, and the bidder shall not use any such for any other purpose.

3.29 Approvals/Clearances

3.29.1 Necessary approvals/ clearances concerned authorities, for establishing the proposed project needs to be obtained by the selected agency.

3.29.2 Necessary approvals/ clearances from concerned authorities, as required, for fire protection, government duties / taxes need to be obtained by the selected bidder.

3.30 Period of Contract and Extension of Work

The GEM Contract will be awarded for initially for 1 year. Based on performance, contract may be extended for 2 years.

3.31 SUPPORT FROM EXTERNAL AGENCY

Sub-letting/contracting of entire work or in part thereof is not permitted. The bidder needs to complete all the defined activities as per scope of work on its own. No Data/ Information should be sent out of the premise without obtaining prior written confirmation from the TENDERER. The successful bidder shall be allowed to obtain advisory support from within its organization towards legal or contractual vetting of drafts.

3.32 USE OF AGREEMENT DOCUMENTS AND INFORMATION

3.32.1 The Bidder shall not without prior written consent from TENDERER disclose the Agreement or any provision thereof or any specification, plans, drawings, pattern, samples, or information furnished by or on behalf of TENDERER in connection therewith to any person other than the person employed by the Bidder in the performance of the Agreement. Disclosure to any such employee shall be made in confidence and shall extend only as far as may be necessary for such performance.

3.32.2 The Bidder shall not without prior written consent of TENDERER make use of any document or information made available for the project except for purposes of performing the Agreement.

3.32.3 All project related documents issued by TENDERER other than the Agreement itself shall remain the property of TENDERER and Originals and all copies shall be returned to TENDERER on completion of the Bidder's performance under the Agreement, if so, required by the TENDERER.

3.33 TAXES & DUTIES

Bidder is liable for all taxes and duties etc. as may be applicable from time to time.

SECTION 4: SCOPE OF WORK (BUT NOT LIMITED TO)

4.1 Red Team Exercise Overview

The objective of a Red Team Exercise is to simulate a real-world attack on an DST/GOG's Projects Such as GSDC, SOC, GSWAN, GISL, GFGNL - IT infrastructure to assess and improve its defences.

Key objectives include:

a. Identifying Vulnerabilities: To discover security gaps that could be exploited by malicious attackers.
b. Testing Incident Response: To evaluate the organization's ability to detect, respond to, and mitigate attacks in real-time.
c. Improving Security Posture: To provide actionable recommendations on how to strengthen the organization's defences against potential threats.
d. Training and Awareness: To help security teams (the "blue team") improve their skills in detecting and responding to real-life attacks.
e. Validating Security Tools: To test the effectiveness of the deployed security tools, firewalls, and monitoring systems against advanced and evolving threats.

4.2 Responsibilities of the Bidder

a. Conduct quarterly Red Team Exercises, or as per the Directive of DST and as and when required.
b. Deploy two (2) qualified resources and all required on-premise automated tool to execute Red Team Exercises at GSDC.
c. Perform the Red Team Exercise using on-premise appliances with minimal internet access.
d. Ensure minimal impact on network performance and should not impact any user flows.
e. The solution/platform should support scaling up to national **remote locations**. (It is considered as DC/DR Sites)
f. The solution/platform should support attack replay and attack import from PCAP.
g. The platform should provide Cyber security dashboard and reports.

4.3 Training and Knowledge Transfer

- Provide training to the identified DST personnel and SOC team on Red Team Exercise, including use case analysis and resolution.

  Conduct mandatory training sessions twice in year, with at least a 6-month gap, for minimum 10 officials.

4.4 Technical Details

Phases of Red Team Exercise

— Initial Compromise
— Establish Foothold
— Lateral Movement
— Complete Mission
— Activities to be Conducted

a. **Reconnaissance**

— Gather information about the Data Center's network, systems, applications, and personnel to identify potential attack vectors.

b. **Enumeration**

— Identify and map all active systems, services, and applications within the network to discover potential vulnerabilities.

c. **Vulnerability Assessment**

— Perform automated and manual vulnerability assessments to identify security weaknesses.

d. **Exploitation**

— Exploit identified vulnerabilities to gain unauthorized access to systems and data, simulating real-world attack scenarios.

e. **Privilege Escalation**

— Attempt to escalate privileges within compromised systems to gain higher levels of access.

f. **Lateral Movement**

— Simulate an attacker's movement within the network to understand the potential impact and spread of a security breach.

g. **Data Exfiltration**

— Attempt to extract sensitive data from the Data Center to test data protection mechanisms and response procedures.

h. **Social Engineering**

— Conduct social engineering attacks, such as phishing and baiting, to test the human element of security.

Deliverables within Red Team Assessment:

Red Team Assessment				
Social Engineering				
Sr. No.	**Descriptions**	**Category**	**Compliance Status (Yes / No)**	**Sample Report Evidence**
1	Impersonation	Social Engineering		
2	Assessing sensitive data exposure	Cloud Security Controls		
3	Phishing Attacks	Email Security Controls		
4	Unauthorized access points	Wireless Security Controls		
5	Web application compromise	Infrastructure & Cloud Security Controls		
6	API security controls	Infrastructure & Cloud Security Controls		
7	Assessing Cloud Exposed Infrastructure	Cloud Security Controls		
8	Tailgating	Physical Security Control		
9	Wireless Access points	Wireless Security Controls		
	• Encryption protocols	Wireless Security Controls		
	• Configuration flaws	Wireless Security Controls		
	• Default Passwords evasion	Wireless Security Controls		
Reconnaissance				
9	Key pointers to be covered on this stage is as follows,	Infrastructure Security Controls		
10	• Identifying reachability of various network segments and gathering detail on them	Infrastructure Security Controls		
11	• Performing Stealth and noisy scan from internal and external environment to understand the preparedness of SOC	Infrastructure Security Controls		
12	• Passive Information gathering on subdomains (internal & external)	Infrastructure Security Controls		

13	• Identifying Gaps and vulnerabilities during recon Phase (external & internal)	Infrastructure Security Controls		
14	• Recon on various handshake / scan mechanism	Infrastructure Security Controls		
15	OSINT	Attack Surface Analysis		
	• Email address	Attack Surface Analysis		
	• Domain names / certificate records	Attack Surface Analysis		
	• Passive DNS	Attack Surface Analysis		
	• residual documents in websites	Attack Surface Analysis		
	• information gathering and potential data pilferage in social media networks like Facebook, Twitter, LinkedIn, GitHub etc.,	Attack Surface Analysis		
	• Metadata from various web platform	Attack Surface Analysis		
	• Information collated from Dark web	Attack Surface Analysis		
	• Typo-squatting	Attack Surface Analysis		
	• Business records leaked in open media like Annual records, employee records, extracting username and email IDs etc.,	Attack Surface Analysis		
Foot printing				
16	Detection of various services / sockets and version details (Ports / network and Vulnerability Scans)	Infrastructure, Endpoint & Cloud Security Controls		
	• Banner grabbing of various platforms without any impact on production	Infrastructure, Endpoint & Cloud Security Controls		
	• Fingerprinting of various HTTP/ HTTPS services (internal / External)	Infrastructure, Endpoint & Cloud Security Controls		
	• Identification of weakness in network, OS, servers, DBs, API, IoT etc.,	Infrastructure Security Controls		
17	• Extracting information using Port scanners (internal / external)	Infrastructure Security Controls		
	o Open	Infrastructure Security Controls		
	o Closed	Infrastructure Security Controls		
	o Filtered	Infrastructure Security Controls		
	o Unfiltered	Infrastructure Security Controls		
	o Open | Filtered	Infrastructure Security Controls		
	o Closed | Filtered	Infrastructure Security Controls		

18	• Using Script scanning to identify Vulnerabilities and associated exploits	Infrastructure, Endpoint & Cloud Security Controls		
19	• Performing various types of scanning like Host Discovery, OS Fingerprinting, Subnet Scanning, Default Scan, Stealth Scan, TCP Scan, UDP Scan, Specific port, Scan ALL port Scan, Version Scan, Script Scan, Decoy Scan, Fast Scan, Time Scan, Aggressive Scan and need to identify vulnerabilities in each form of scans and should apprise earnestly for fixing security weakness	Infrastructure, Endpoint & Cloud Security Controls		
Enumeration & Exploitation				
20	Various process of enumeration has to be carried out to find weakness in the system as per testers approach and also not withstanding to the following points (wherever applicable),	Infrastructure Security Controls		
	• Extracting information using default passwords	Infrastructure, Endpoint & Cloud Security Controls		
	• Brute force Active Directory	Infrastructure, Endpoint & Cloud Security Controls		
	• Extract information for LDAP	Infrastructure, Endpoint & Cloud Security Controls		
	• Extract information using SNMP / SNMP trap	Infrastructure, Endpoint & Cloud Security Controls		
	• Extract information using DNS zone transfer	Infrastructure, Endpoint & Cloud Security Controls		
	• Extract information using SMTP	Infrastructure, Endpoint & Cloud Security Controls		
	• Extract information using SMB	Infrastructure, Endpoint & Cloud Security Controls		
	• extract information using Microsoft RPC	Infrastructure, Endpoint & Cloud Security Controls		
	• Extract information using NetBIOS / NBNS	Infrastructure, Endpoint & Cloud Security Controls		
	• Extract information using NTP enumeration	Infrastructure, Endpoint & Cloud Security Controls		
21	The exploiting Phase should be carried-out in controlled environment without impacting production. Apart from the testers-way of exploiting the following activity should also be carried out to check the effectiveness of the Security posture,	Infrastructure, Endpoint & Cloud Security Controls		
	o Post Enumeration Gathering System information	Infrastructure, Endpoint & Cloud Security Controls		

	o Gathering User Information	Infrastructure, Endpoint & Cloud Security Controls		
	o Download and Upload operations	Infrastructure, Endpoint & Cloud Security Controls		
	o Process Migrate	Infrastructure, Endpoint & Cloud Security Controls		
	o Collect Stored Credentials (System, Brower, Wifi)	Infrastructure, Endpoint & Cloud Security Controls		
	o Privilege Escalation to gain Administrator Access	Infrastructure, Endpoint & Cloud Security Controls		
	o Hash dump	Infrastructure, Endpoint & Cloud Security Controls		
	o Clear Event logs	Infrastructure, Endpoint & Cloud Security Controls		
	o Persistence to maintain permanent access	Infrastructure, Endpoint & Cloud Security Controls		
22	Finding the options for lateral movement by various methods and not restricting to the following	Infrastructure, Endpoint & Cloud Security Controls		
	• Bypassing Windows User Account Control	Infrastructure, Endpoint & Cloud Security Controls		
	• Windows UAC Bypass	Infrastructure, Endpoint & Cloud Security Controls		
	• Fileless UAC bypass	Infrastructure, Endpoint & Cloud Security Controls		
	• PowerShell enumeration	Infrastructure, Endpoint & Cloud Security Controls		
	• bypassing IDS / IPS	Infrastructure, Endpoint & Cloud Security Controls		
	• Malware Cloaking using Digital Steganography	Infrastructure, Endpoint & Cloud Security Controls		
	• Active directory Default local Accounts enumeration	Infrastructure, Endpoint & Cloud Security Controls		
	• Golden Ticket attack	Infrastructure, Endpoint & Cloud Security Controls		
23	• Man-in-the-middle attack not restricting to the following methods,	Infrastructure, Endpoint & Cloud Security Controls		
	o ARP spoofing	Infrastructure, Endpoint & Cloud Security Controls		
	o Bypassing HTTPS	Infrastructure, Endpoint & Cloud Security Controls		
	o Session hijacking	Infrastructure, Endpoint & Cloud Security Controls		
	o code injection	Infrastructure, Endpoint & Cloud Security Controls		
	o DNS Spoofing	Infrastructure, Endpoint & Cloud Security Controls		
	o IP Spoofing	Infrastructure, Endpoint & Cloud Security Controls		
	o MAC spoofing	Infrastructure, Endpoint & Cloud Security Controls		
Persistence				
24	The tester should identify and validate the capability of persistence and data exfiltration that should also include	Infrastructure, Endpoint & Cloud Security Controls		

	• Gaining domain Admin	Infrastructure, Endpoint & Cloud Security Controls		
	• Gaining system /device admin	Infrastructure, Endpoint & Cloud Security Controls		
	• evading Antivirus	Endpoint Security Controls		
	• evading EDR	Endpoint Security Controls		
	• erasing security logs	Infrastructure, Endpoint & Cloud Security Controls		
	• re-writing security logs	Infrastructure, Endpoint & Cloud Security Controls		
	• re-writing security logs on stopping AV	Endpoint Security Controls		
	• Covert channel Data exfiltration using DNS Tunnelling	Infrastructure, Endpoint & Cloud Security Controls		
	• PHP evasion	Infrastructure Security Controls		
	• Horizontal Privilege escalation	Infrastructure Security Controls		
	• Vertical Privilege escalation	Infrastructure Security Controls		
	• PowerShell exploitation	Infrastructure Security Controls		
	• Evasion and obfuscation techniques	Infrastructure Security Controls		
	• DDoS / flooding - network traffic jamming	Infrastructure Security Controls		
	• Supply Chain attack	Infrastructure Security Controls		
	• FTP / telnet Password capture	Infrastructure Security Controls		
	• Cryptographic attacks	Infrastructure Security Controls		
	• Honey pots / DMZ	Infrastructure Security Controls		
	And testify data exfiltration by various methods including the following	Infrastructure Security Controls		
	• Exfiltration using netcat	Infrastructure Security Controls		
	• Exfiltration using SSH	Infrastructure Security Controls		
	• Exfiltration using Wget	Infrastructure Security Controls		
	• DLP sensor evasion	Endpoint Security Controls		

- It is expected that the Bidder to execute the above deliverables in quarterly and define milestones for each quarter.

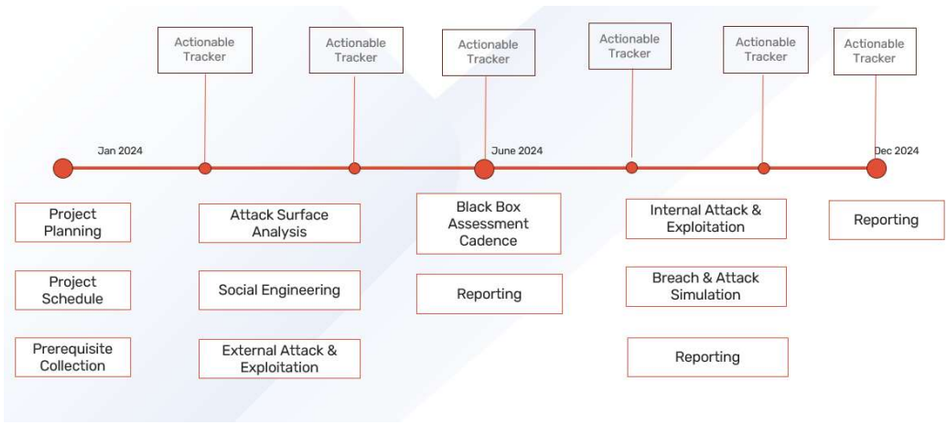
Expected mapping for deliverables with objectives and milestones is stated as follows:

Quarter	**Objective**	**Description**	**Scope Covered**	**Key Activities**	**Milestones**
Q1	• To determine external digital attack surface of the organization. • To determine gaps from physical and	To attain the objective, open-source intelligence activity would be performed to gaze the attack surface of the organization infrastructure.	• External Attack Surface Analysis • Physical Controls • Wireless Controls	Metadata from various web platform Information collated from Dark web Tailgating	• External Attack Surface Analysis • Physical Controls • Wireless Controls

	wireless controls perspective.	Domain and Employee lookup would be performed on the Dark Web as well. Apart from this wireless attack and exploitation would be performed on the Guest AP to determine if other interfaces can be enumerated.		Unauthorized access points	
Q2	• To perform phishing on the scrapped information from last phase. • To determine gaps in email security controls. • To determine gaps in cloud security controls. • To identify exploitable vulnerabilities onto discovered external attack surface.	To attain the objective, email scrapping technique used in the previous phase would serve as a output to this phase. Phishing would be performed on the IDs for payload delivery. Within this the email security controls would also be checked. In this phase we would also be identifying exploitable vulnerabilities that would help an attacker to get into the customer infrastructure. The activity would be carried on organization's exposed cloud services, applications, APIs, etc.	• Phishing • Cloud Security Controls • External Attack Exploitation - Web, Mobile, API	Assessing Cloud Exposed Infrastructure Impersonation Assessing sensitive data exposure Web application compromise	• Phishing • Cloud Security Controls • External Attack Exploitation - Web, Mobile, API
Q3	• To determine gaps in endpoint security controls. • To identify exploitable vulnerabilities onto discovered internal attack surface.	To attain the objective, we would be requiring a machine within the customer infrastructure. The machine would have all the security controls implemented into it. The objective would be to bypass the security controls and move laterally within the infrastructure to determine exploitable vulnerabilities into	• Endpoint Security Controls • Internal Attack Exploitation - Web, Mobile, Database, API	Extract information using SMB Extract information using Microsoft RPC Extract information using NetBIOS / NBNS	• Endpoint Security Controls • Internal Attack Exploitation - Web, Mobile, Database, API

		the internal infrastructure.			
Q4	• To perform Breach & Attack Simulation	To attain the objective, threat profiling would be performed in conjunction with global threat intelligence to create different campaigns and perform simulation of the techniques from MITRE ATT&CK framework perspective.	• Breach & Attack Simulation	Threat Profiling TTP Simulation	• Breach & Attack Simulation

- For the above milestone based it is expected that the bidder should comply to below project plan of duration of 1 Year. The start date and end action are taken just for reference. Actual start and end date would vary upon award of the project.



- Bidder should provide detailed “Rules of Engagement” document before initiating the project. Bidder is required to submit sample Rules of Engagement as part of evidence.
- Bidder should take into consideration of all the necessary authorizations, attestation, Indemnity required to initiate the project.
- Bidder to comply with MITRE ATT&CK framework and NIST SP 800-115.
- Red Team results shall be documented using open, machine-readable standards (e.g., SCAP)
- Bidder should devise a scoring method for determining the results Red Team exercises so that results can be compared over time.
- Bidder should execute at least minimum 12 Cyber Kill Chains / APT Groups during entire year. With 1 APT execution or Cyber Kill Chain execution in each month.
- Bidder will be providing a platform from where reports can be downloaded and observations can be viewed.
- Bidder will be providing a platform from where reports of red teaming and breach and attacking simulation can be downloading the report and also provide a dashboard which would have following parameters – MITRE ATT&CK Mapping, Attack flows which are incorporated from Centre of Threat Informed Defense. Bidder is requested to submit the screenshot of the dashboard as part of evidence.
- Bidder to perform Breach & Attack Simulation with an automated tool which includes Ransomware Simulation and support detection engineering. The tool will be executing in continuous manner throughout the year.
- Bidder should have the capability to perform and demonstrate manual Security Control Validation using commercial C2 frameworks like CobaltStrike, BRC4.
- Bidder should achieve below goals as part of the engagement:
    - Compromising Critical User
    - Compromising Critical Asset

    - Gaining access to Domain Controller
    - Data Exfiltration
    - EDR Evasion
- Bidder should provide insights on the exposed credentials on the dark web and should use to link into cyber kill chain.
- Bidder is required to perform continuous dark web monitoring for a period of one year to understand the leaks on dark web and use the information within red teaming. Bidder is required to submit evidence of continuous dark web monitoring and its utilization in Red Teaming.
- Bidder should provide insights on the leaks and should use to link into cyber kill chain.
- Bidder should perform Physical Security to perform below attacks:
    - Tailgating
    - Access Card Cloning
    - WiFi Compromise
- Bidder should provide recommendations in below categories:
    - Code / Infra Fixes
    - Detective Control Fine Tuning
    - Preventive Control Fine Tuning
- Bidder should have a perform consultative calls with SOC team to improve Rule Optimization within SIEM.

Bidder is required to have Quarterly Review Sessions where a senior resource, apart from 2 deployed resources is required to come onsite and demonstrate the presentation on the overall status of the engagement.

4.4.1 Deliverables

- As part of Deliverables, Bidder is expected to include below pointers:
- Below are the deliverables which would be provided after the engagement.
    - Execution Plan with detailed explanation phase wise.
    - Executive Summary – Executive level summary report that provides an overview of the project scope, key findings, business risks and impacts, associated root causes and key recommendations.
    - Detailed Technical Findings Report – An in-depth detailed technical report intended for the client's technical staff that documents the following:
        - The step-by-step path of how we obtained unauthorized access in both narrative and illustrative formats.
        - A detailed findings matrix that documents an overview of each identified vulnerability, its risk rating, impact and technical remediation recommendation
        - Proof of concept providing evidence and/or exploitation steps of the vulnerability
        - Mitigation / Solution techniques for reported security vulnerabilities.
    - Bidder is to be required to submit reports based upon milestone bases. The milestone reports includes – Black Box Report, Assumed Breach Report, Breach & Attack Simulation Report.
    - Bidder is also required to submit executive report which includes overall risk score of the organization along with cyber kill chain. Bidder is required to submit sample executive report as part of evidence.
    - To deliver the complete project, Bidder is required to deploy minimum 2 onsite resource for the complete year to achieve the objectives defined in the RFP and derived in Rules of Engagement.

- **Initial Assessment Report**
    - A preliminary report outlining the initial findings, methodologies used, and identified vulnerabilities.
- **Final Assessment Report**
    - A comprehensive report detailing all findings, including the severity and impact of identified vulnerabilities, exploitation methods, and the potential risks.
- **Remediation Recommendations**
    - Detailed recommendations for mitigating identified vulnerabilities, categorized by priority and criticality.
- **Executive Summary**

    - A high-level summary of the findings and recommendations, suitable for presentation to senior management and stakeholders.
- **Debriefing Sessions**
    - Conduct debriefing sessions with relevant stakeholders to discuss the findings, recommendations, and next steps for remediation.

4.4.1.1 Detailed Reports

After each Red Team Exercise, deliverables in relation to the analysis should be reported to the GSOC within 15 days of completion, covering the following aspects:

1. **Security Gaps**
    - Detailed system setup and tools used.
    - Analysis and documentation of security gaps.
    - Recommendations for addressing security gaps.
    - Roadmap for compliance and addressing security gaps.
2. **Addressing Security Gaps**
    - Actionable fixes for vulnerabilities.
    - Suggested changes in security policies and architecture.
    - Compensatory controls if risk mitigation cannot be implemented.
3. **Summary Report**
    - Findings, tools used, positive security aspects, list of vulnerabilities.
    - Description and risk rating of vulnerabilities.
    - Methodology and test cases used, impact analysis, and recommendations.

4.4.2 Technical Requirements

4.4.2.1 Platform Capabilities

- Support for scaling to national and international locations.
- Ability to create custom attacks and import PCAP.
- Integration with vulnerability management systems.
- Non-destructive testing in production environments.
- Detailed attack simulation dashboards (e.g., MITRE Attack, Heatmap).

4.4.2.2 Compliance and Standards

- Adherence to prevailing guidelines, IT Act, and other applicable regulations in India.
- Testing in accordance with global best practices.

SECTION 5: PENALTIES AND SERVICE LEVEL AGREEMENT (SLA)

The purpose of this Service Level Agreement (hereinafter referred to as SLA) is to clearly define the levels of service which shall be provided by SUCCESSFUL BIDDER to the CLEINT for the duration of this contract period of the Project.

All the payments related to the warranty period to the selected bidder referred to as “agency” are linked to the compliance with the SLA metrics specified in this document. Penalty levied for non-performance as per SLA requirements shall be deducted from subsequent payments due or from the Performance Bank Guarantee submitted by the bidder. The maximum ceiling of penalty shall be up to 20 percent (%) of the total contract value.

5.1 Implementation Timeline & Penalties

The Red Team Exercise timeline defines key deliverables and corresponding penalties for delays in submission or execution. The Vendor is required to adhere to the following timelines for deliverables:

S/N	Measurement	Target	Penalty for Delay
1	**Kick-off Meeting**	2 weeks from issuance of GEM contract	₹50,000 per week or part thereof. Delays exceeding 4 weeks may result in contract termination and forfeiture of PBG.
2	**Training Sessions**	T1 = T + 4 weeks	₹20,000 per session per week of delay.
3	**Red Team Assessment Execution**	T2 = T1 + 4 weeks	2% of the Quarterly payment per week of delay, capped up to 10% of the quarterly payment. Delays beyond 12 weeks may lead to contract termination.
4	**Submission of Red Team Reports (as defined above)**	Within 15 days post-assessment	2% of Quarterly payment per day of delay, capped at 10% of the quarterly payment.

T = Date of Award of GEM Contract

S/N	Deliverable
1	**Pre-Exercise Briefing Document**
2	**Red Team Assessment Reports**
3	**Technical Findings Report**
4	**Executive Summary Report**
5	**Post-Exercise Debriefing Report**
6	**Training Session Reports**

Note:

- Quarterly Payment will be made after submission of aforementioned all deliverables within 30 days of completion of quarterly exercise.
- Successful Bidder shall be paid Quarterly Payment (QP) as per the services provided to TENDERER. The overall penalty would be calculated cumulatively & it will be generally capped at 10% of QP amount. If the cap of overall penalty is reached in two consecutive Quarter, the penalty cap for the third Quarter onwards, for each Quarter will increase by 5% over the penalty cap for the preceding quarterly till it reaches 25% of the QP. In addition to the applicable penalty and the provisions pertaining to closure/termination of contract, the TENDERER shall be within its rights to undertake termination of contract if or anytime the penalty increases by 15% of the QP. Once the penalty cap has increased beyond 10%, if the bidder through better performance delivery for any Quarter, brings the leviable penalty below 10% then the computation of the 1st of the 2 consecutive Quarter as referred above will reset and will begin afresh.
- During contract period, if tenderer asked any report bidder has to submit those reports within timeline as mentioned in this RFP.

5.2 Performance Metrics

The Vendor is expected to meet the following performance standards:

- **Accuracy of Reports**: Reports must accurately reflect the findings of the Red Team Exercise, including vulnerabilities, their criticality, and recommended remediation steps.
- **Completeness**: All reports must include detailed technical analysis, risk ratings, and evidence of exploitation or proof-of-concept.
- **Compliance with Standards**: The Vendor must ensure compliance with relevant industry standards such as MITRE ATT&CK, NIST, and other security frameworks as published by CERT-IN, GOI.
- **Timely Communication**: The Vendor is required to communicate any potential delays in deliverables well in advance and propose corrective actions to minimize the impact as mentioned in this RFP.

5.3 Resolution of Complaints

9.6.1 Any complaints (other than the SLA parameters) notified by the Authority to the Agency shall have to be replied to in written along with the suggested course of action to be taken in order to resolve the complaint by the Agency within 10 (ten) working days of the complaint being notified.

9.6.2 The suggested course of action by the Agency shall then be reviewed by the Authority and the final modifications (if any) shall have to be implemented in a manner and time frame suggested by the Authority.

5.4 Force Majeure

9.7.1 Force Majeure shall mean any event beyond the control of Authority or of the Agency, as the case may be, and which is unavoidable notwithstanding the reasonable care of the party affected, and which could not have been prevented by the exercise of reasonable skill and care and good industry practices and shall include, without limitation, the following:

a. War, hostilities, invasion, acts of a foreign enemy and civil war.
b. Rebellion, revolution, insurrection, mutiny, conspiracy, riot, civil commotion, and terrorist acts.
c. Strike, sabotage, unlawful lockout, epidemics, quarantine, and plague.
d. Earthquake, fire, flood or cyclone, or other natural disaster
e. Any other event as decided by the Authority

9.7.2 As soon as reasonably practicable but not more than 48 (forty-eight) hours following the date of commencement of any event of Force Majeure, an Affected Party shall notify the other Party of the event of Force Majeure setting out, inter alia, the following in reasonable detail:

a. The date of commencement of the event of Force Majeure.
b. The nature and extent of the event of Force Majeure.
c. The estimated Force Majeure Period,
d. Reasonable proof of the nature of such delay or failure and its anticipated effect upon the time for performance and the nature of and the extent to which, the performance of any of its obligations under the Agreement is affected by the Force Majeure.
e. The measures which the Affected Party has taken or proposes to take to alleviate/mitigate the impact of the Force Majeure and to resume the performance of such of its obligations affected thereby.
f. Any other relevant information concerning the Force Majeure and/or the rights and obligations of the Parties under the Agreement.

SECTION 6: Payment Terms

The payment for services rendered under the Red Team Exercise RFP will be released in a phased manner after completion of **Completion of Quarterly Red Team Assessment with all necessary Report Submissions which are asked in this RFP.**

Notes:

- No advance payment will be made.
- Invoice should be generate in name of Security Operations Center, Directorate of ICT & e-Governance.
- Invoice should be submitted with all reports and necessary artifacts. payment will be processed after submission of all necessary documents.
- All payments will be subject to penalties for delays, as specified in the **Service Level Agreement (SLA).**
- In case of any penalties applied due to delays or non-compliance with SLAs, the corresponding deductions will be made before processing payments.
- For all above mentioned activities for Red Team Exercise Necessary Manpower compulsorily need to be deployed at GSDC.

SECTION 7: FINANCIAL BID FORMAT

The bidder shall submit the commercial bid in the below format.

Service Description	Quantity (Quarters)	Total with Taxes
Red Teaming Assessment as per the Tender Scope (every quarter for 1 Year)	4	

Note:

i. L1 will be the lowest sum total of rates of all line items including GST.
ii. User Department/GIL may negotiate the prices with L1 Bidder, under each item/head offered by Bidder.
iii. The Bidder needs to quote the price inclusive of GST in the financial bid. Any changes in GST duties would be applicable as on actual at the time of invoice processing.
iv. Above table will be used for Commercial Bid evaluation purpose only. The Bidder should not upload the financial document along with the technical document, if found, the bid of respective bidder shall be summarily rejected.
v. The Contract will be awarded for 1 year to successful bidder, based on bidder performance, Department may extend the contract for next 02 years.

SECTION 8: ANNEXURES & FORMATS

8.1 Format 1: Proposal Covering Letter

(To be on the Bidder's letterhead duly Signed by Authorized Signatory)

Tender Ref No:

To
Deputy General Manager (Technical)
Gujarat Informatics Ltd.
Block no. 2, 2nd floor, Karmayogi Bhavan,
Sector 10-A, Gandhinagar.

Ref: <RFP Title>.

Dear Sir,

We …… (Name of the bidder) hereby submit our proposal in response to notice inviting tender date ……. And tender document no. xxxxxxxxxx Dated: dd/mm/yyyy and confirm that:

1. All information provided in this proposal and in the attachments, is true and correct to the best of our knowledge and belief.
2. We shall make available any additional information if required to verify the correctness of the above statement.
3. Certified that the period of validity of bids is 180 days from the last date of submission of proposal, and
4. We are quoting for all the items (including services) as per the price bid format Section-VII as mentioned in the RFP.
5. We the Bidder are not under a declaration of Ineligibility for corrupt or fraudulent practices or blacklisted by any of the Government agencies.
6. We have an office in the state and relevant documents for the same are attached. We undertake that if the local presence is not there in the state, that we shall establish an office at Gandhinagar/ Ahmedabad, within 45 days from the date of the award of contract.
7. Gujarat Informatics Limited may contact the following person for further Information regarding this tender: -
    a. Name & Designation:
    b. Full address of office
    c. Email ID & Contact No.
8. We are uploading our Response to the RFP (Eligibility, technical and financial bid documents) as per the instructions set out in this RFP.

Yours Sincerely,

(Signature)

Name of Authorized Signatory:
Designation:
Date:
Name of the bidder:

8.2 Format 2: Bank Guarantee format for Earnest Money Deposit

To Dated:

Deputy General Manager (Technical)
Gujarat Informatics Ltd
Block no. 2, 2nd floor, Karmayogi Bhavan,
Sector-10A, Gandhinagar.

Whereas ---------- (here in after called "the Bidder") has submitted its bid dated ---------- in response to the Tender no: xxxxxxxxxxxxxxxxxx for _____ KNOW ALL MEN by these presents that WE ---------- having our registered office at ---------- (hereinafter called "the Bank") are bound unto the _____, Gujarat Informatics Limited in the sum of ---------- for which payment well and truly to be made to Gujarat Informatics Limited , the Bank binds itself, its successors and assigns by these presents. Sealed with the Common Seal of the said Bank this ----------day of ----------2023.

THE CONDITIONS of this obligation are:

The EMD may be forfeited, In case of a Bidder if:

1) The bidder withdraws its bid during the period of bid validity.
    a. The Bidder does not respond to requests for clarification of their Bid.
    b. The Bidder fails to co-operate in the Bid evaluation process.
    c. The bidder, fails to furnish Performance Bank Guarantee in time.
2) The bidder fails to Sign the contract in accordance with this RFP
3) The bidder is found to be involved in fraudulent and corrupt practices

We undertake to pay to the GIL up to the above amount upon receipt of its first written demand, without GIL having to substantiate its demand, provided that in its demand GIL will specify that the amount claimed by it is due to it owing to the occurrence of any of the above-mentioned conditions, specifying the occurred condition or conditions.

This guarantee will remain valid up to 9 months from the last date of bid submission. The Bank undertakes not to revoke this guarantee during its currency without previous consent of the GIL and further agrees that the guarantee herein contained shall continue to be enforceable till the GIL discharges this guarantee The Bank shall not be released of its obligations under these presents by any exercise by the GIL of its liability with reference to the matters aforesaid or any of them or by reason or any other acts of omission or commission on the part of the GIL or any other indulgence shown by the GIL or by any other matter or things.
The Bank also agree that the GIL at its option shall be entitled to enforce this Guarantee against the Bank as a Principal Debtor, in the first instance without proceeding against the SELLER and not withstanding any security or other guarantee that the TENDERER may have in relation to the SELLER's liabilities.
Dated at _____ on this _____ day of _____2025.

Signed and delivered by

_____
For & on Behalf of
Name of the Bank & Branch &
Its official Address with seal

Approved Bank: All Nationalized Bank including the public sector bank or Private Sector Banks or Commercial Banks or Co-Operative & Rural Banks (operating in India having branch at Ahmedabad/ Gandhinagar) as per the G.R. no. FD/MSM/e-file/4/2023/4020/D.M.O. dated 11.03.2024 issued by Finance Department or further instruction issued by Finance department time to time.

8.3 Format 3: PERFORMANCE BANK GUARANTEE

(To be stamped in accordance with Stamp Act)

Ref: Bank Guarantee No.
Date:

To,
Deputy General Manager (Technical)
Gujarat Informatics Ltd.
Block no. 2, 2nd floor, Karmayogi Bhavan,
Sector-10A, Gandhinagar.

Dear Sir,

WHEREAS..... (Name of Bidder) hereinafter called "the Bidder" has undertaken, in pursuance of Agreement dated, (hereinafter referred to as "the Agreement for "RFP regarding empanelment of agencies for **<Tender Title>, (Tender No. xxxxxxxxxxxxxxxx Dated: xx.xx.xxxx)** for the Department of Science & Technology, Government of Gujarat.

AND WHEREAS it has been stipulated in the said Agreement that the Bidder shall furnish a Bank Guarantee ("the Guarantee") from a scheduled bank for the sum specified therein as security for implementing PROJECT.

1. WHEREAS we _____ ("the Bank", which expression shall be deemed to include it successors and permitted as Signs) have agreed to give the Gujarat Informatics Limited ("GIL") the Guarantee:

THEREFORE, the Bank hereby agrees and affirms as follows:

The Bank hereby irrevocably and unconditionally guarantees the payment of all sums due and payable by the Bidder to GIL under the terms of their Agreement dated _____. Provided, however, that the maximum liability of the Bank towards GIL under this Guarantee shall not, under any circumstances, exceed _____ in aggregate.

2. In pursuance of this Guarantee, the Bank shall, immediately upon the receipt of a written notice from GIL in that behalf and without delay/demur or set off, pay to GIL any and all sums demanded by GIL under the said demand notice, subject to the maximum limits specified in Clause 1 above. A notice from GIL to the Bank shall be sent by Registered Post (Acknowledgement Due) at the following address:

_____
_____
_____
Attention Mr. _____.

3. This Guarantee shall come into effect immediately upon execution and shall remain in force for a period of months from the date of its execution. The Bank shall extend the Guarantee for a further period which may be mutually decided by the bidder and GIL.

The liability of the Bank under the terms of this Guarantee shall not, in any manner whatsoever, be modified, discharged, or otherwise affected by:

- Any change or amendment to the terms and conditions of the Contract or the execution of any further Agreements.
- Any breach or non-compliance by the Bidder with any of the terms and conditions of any Agreements/credit arrangement, present or Future, between Bidder and the Bank.

4. The BANK also agrees that GIL at its option shall be entitled to enforce this Guarantee against the Bank as a Principal Debtor, in the first instance without proceeding against the BIDDER and not withstanding any security or other guarantee that GIL may have in relation to the Bidder's liabilities.

5. The BANK shall not be released of its obligations under these presents by reason of any act of omission or commission on the part of GIL or any other indulgence shown by GIL or by any other matter or thing whatsoever which under law would, but for this provision, have the effect of relieving the BANK.

6. This Guarantee shall be governed by the laws of India and the courts of Gandhinagar shall have jurisdiction in the adjudication of any dispute which may arise hereunder.

Dated this ……. Day of ……..,2025

Witness

(Signature)
(Name)

(Official Address)

(Signature)
Bank Rubber Stamp
(Name)
Designation with Bank Stamp
Plus, Attorney as per Power of Attorney No.

Dated:

Approved Bank: All Nationalized Bank including the public sector bank or Private Sector Banks or Commercial Banks or Co-Operative & Rural Banks (operating in India having branch at Ahmedabad/ Gandhinagar) as per the G.R. no. FD/MSM/e-file/4/2023/4020/D.M.O. dated 11.03.2024 issued by Finance Department or further instruction issued by Finance department time to time.

8.4 Format 4: Format for Financial Summary of the Bidder

(Same should be furnished by the Charted Accountant / Statutory Auditor on their letter head)

Average Annual Turnover of the Bidder (from works related to providing Web, Mobile and Software Development)

S. No	Financial Year	Annual Turnover (INR)
1.		
2.		
3.		
	[Average Annual Turnover]	**[indicate sum of above divided by 3]**

Note: Bidders are required to provide data for last three years ending 31st March 2023. Audited Balance Sheets are also required to be submitted for the same.

UDIN No:_____

Certificate from the Statutory Auditor

Note:

1. The Bidder shall submit audited annual reports (financial statements: balance sheets, profit and loss account, notes to accounts etc.) in support of the financial data duly certified by statutory auditor/s. In case, the company does not have a statutory auditor/s, it shall be certified by the chartered accountant that ordinarily audits the annual financials of the company.
2. Certificate(s) from the statutory auditors specifying the Turnover of the Bidder, as on FY 2020-21, OR FY 2021-22 OR FY 2022-23 (as the case may be). For the purpose of this RFP, net worth shall mean the sum of subscribed and paid-up equity share capital and reserves from which shall be deducted the sum of revaluation reserve, miscellaneous expenditure not written off and reserves not available for distribution to equity shareholders.

8.5 Format 5: SELF DECLARATION

(TO BE SUBMITTED PHYSICALLY ALONG WITH EMD)

AFFIDAVIT

(To be submitted IN ORIGINAL on Non-Judicial Stamp Paper of Rs 300/- duly attested by First Class Magistrate/ Notary public)

I/We, _____, age_____ years residing at _____ in capacity of _____M/s. _____ hereby solemnly affirm that

All General Instructions, General Terms and Conditions, as well as Special Terms & Conditions laid down on all the pages of the Tender Form, have been read carefully and understood properly by me which are completely acceptable to me and I agree to abide by the same.

I I We have submitted following Certificates I Documents for T.E. as required as per General Terms & Conditions as well as Special Terms & Conditions of the tender

Sr. No.	Name of the Document
1	
2	

All the Certificates I Permissions I Documents I Permits I Affidavits are valid and current as on date and have not been withdrawn I cancelled by the issuing authority.

It is clearly and distinctly understood by me that the tender is liable to be rejected if on scrutiny at any time, any of the required Certificates I Permissions I Documents I Permits I Affidavits is I are found to be invalid I wrong I incorrect I misleading I fabricated I expired or having any defect.

I I We further undertake to produce on demand the original Certificate I Permission I Documents I Permits for verification at any stage during the processing of the tender as well as at any time asked to produce.

I I We also understand that failure to produce the documents in "Prescribed Performa" (wherever applicable) as well as failure to give requisite information in the prescribed Performa may result in to rejection of the tender.

My I Our firm has not been banned I debarred I black listed at least for three years (excluding the current financial year) by any Government Department I State Government I Government of India I Board I Corporation I Government Financial Institution in context to purchase procedure through tender.

I I We confirm that I I We have meticulously filled in, checked and verified the enclosed documents I certificates I permissions I permits I affidavits I information etc. from every aspect and the same are enclosed in order (i.e. in chronology) in which they are supposed to be enclosed. Page numbers are given on each submitted document. Important information in each document is "highlighted" with the help of "marker pen" as required.

The above certificates/ documents are enclosed separately and not on the Proforma printed from tender document.

I I We say and submit that the Permanent Account Number (PAN) given by the Income Tax Department is _____, which is issued on the name of _____ [Kindly mention here either name of the Proprietor (in case of Proprietor Firm) or name of the tendering firn;1, whichever is applicable].

I I We understand that giving wrong information on oath amounts to forgery and perjury, and I/We am/are aware of the consequences thereof, In case any information provided by us are found to be false or incorrect, you have right to reject our bid at any stage including forfeiture of our EMD/PBG/cancel the award of contract. In this event, this office reserves the right to take legal action on me/us.

I / We have physically signed &stamped all the above documents along with copy of tender documents (page no. ---- to --).

I I We hereby confirm that all our quoted items meet or exceed the requirement and are absolutely compliment with specification mentioned in the bid document.

My I Our Company has not filed any Writ Petition, Court matter and there is no court matter filed by State Government and its Board Corporation, is pending against our company .

I / We hereby commit that we have paid all outstanding amounts of dues/ taxes/ cess/ charges/ fees with interest and penalty.

In case of breach of any tender terms and conditions or deviation from bid specification other than already specified as mentioned above, the decision of Tender Committee for disqualification will be accepted by us.

Whatever stated above is true and correct to the best of my knowledge and belief.

Date: Stamp & Sign of the Tenderer

Place: (Signature and seal of the Notary)