SECURITIES AND EXCHANGE BOARD OF INDIA

REQUEST FOR PROPOSAL

FOR

SEBI Enterprise-wide Integrated IT Network Infrastructure

(SIT-NET)

RFP No. SEBI /ITD/HO/2020/12/02

This is a confidential document and is the property of Securities and Exchange Board of India (SEBI). It may not be copied, distributed or recorded on any medium, electronic or otherwise, without SEBI's prior written permission. The use of the contents of this document, even by the authorized personnel / agencies for purposes other than the purpose specified herein, is strictly prohibited and in case of any violation of this stipulation, SEBI may initiate action under applicable civil and criminal laws.

Table of Contents

Disclaimer & Disclosures

a) The information contained in this Request for Proposal ("RFP / Bid Document") or information provided subsequently to bidder(s) or vendor(s) in documentary form by or on behalf of SEBI, is provided to the bidder(s) on the terms and conditions set out in this RFP document and all other terms and conditions subject to which such information is provided. All communication with regard to RFP will be in written format only.

b) The information in this RFP is to facilitate the Bidders to propose suitable, cost effective solution. However, Bidders are required to make their own inquiries and will be required to confirm that they have done so and they do not rely only on the information provided by SEBI in submitting response to the RFP document. The information is provided on the basis that it is non–binding on SEBI or any of its authorities, agencies, officers, employees, agents or advisers. SEBI reserves the right not to proceed with the Project or to change the configuration of the Project, to alter the time table reflected in this document or to change the process or procedure to be applied. No reimbursement of cost of any type will be paid to persons or entities participating in the process.

c) Any product name / function used in this document are meant to be generic and do not refer to the product of any particular company. In case such proprietary terms have been inadvertently mentioned then such terms should be taken to refer to the generic technology(ies). Bidders with industry standard equivalent product name / function under any other name will also be eligible to submit their bids.

d) This RFP document is not an agreement and is neither an offer. The purpose of this RFP is to provide applicants who are short listed to submit the bids ("Bidders") with information to assist them in formulation of their proposals ("Bids"). This RFP does not claim to contain all the information each Bidder may require. Each Bidder may conduct its own independent investigations and analysis and is free to check the accuracy, reliability and completeness of the information in this RFP. SEBI makes no representation or warranty, express or implied, and shall incur no liability whatsoever under any law, statute, rules or regulations as to the accuracy, reliability or completeness of this RFP. SEBI may in its absolute discretion, but without being under any obligation to do so, update, amend or supplement the information in this RFP.

e) SEBI reserves the right to reject any or all the responses to the RFP. Bids received in response to this RFP at any stage without assigning any reason whatsoever and without being liable for any loss/injury that Bidder might suffer due to such reason. The decision of SEBI shall be final, conclusive and binding to all the parties directly or indirectly connected with the bidding process.

f) It may be noted that notice regarding corrigenda, addendum, amendments, time-extensions, clarifications, response to bidders' queries etc., if any to RFP, will not be published through any advertisement in newspapers or any other media. The same shall be communicated to the shortlisted bidders through email/SEBI website.

DEFINITIONS

“Acceptance” means SEBI’s written certification that the Systems (or a specific part thereof) installed have been tested and verified as complete and fully operational in accordance with the acceptance details, as specified in this RFP;

"Acceptance Certificate" means certificate issued by SEBI only after clearance of all outstanding issues relating to Acceptance;

"Acceptance Test" or "Acceptance Testing" means the testing of the Systems (or a specific part thereof) installed to verify if the Systems are complete and fully operational in accordance with the Acceptance.

“Agreement” means the agreement entered into between the SEBI and the Solution Partner, as recorded and signed by the parties, including all attachments and annexure thereto and all documents incorporated by reference therein;

“Application Software” means business or technical software, either packaged or custom-developed using Standard Software, formulated to interface with the users of the data processing system;

"Annual Maintenance Contract" means the annual contract governing the maintenance of the Solution provided by the Solution Partner, after the Warranty Period;

“Business Day” means day on which SEBI conducts regular business;

"Computer" means any electronic magnetic, optical or other high-speed data processing device or system which performs logical, arithmetic, and memory functions by manipulations of electronic, magnetic or optical impulses, and includes all input, output, processing, storage, computer software, or communication facilities which are connected or related to the computer in a computer system or computer network;

“Custom Software” means the software specifically and exclusively developed by the Solution Partner for SEBI in terms of this RFP and includes any modifications made thereto from time to time;

“Day” means calendar day;

“Data” means a representation of information, knowledge, facts, concepts or instructions which are being prepared or have been prepared in a formalised manner, and is intended to be processed, is being processed or has been processed in a computer system or computer network, and may be in any form (including computer printouts magnetic or optical storage media, punched cards, punched tapes) or stored internally in the memory of the computer;

"Data Centre" means such place designated by SEBI as a server room for hosting the solution proposed by Solution Partner.

“Deliverable” means the Solution provided by the Solution Partner of the tasks stated in the Project Plan;

“Deployment of Resources” means

“Effective Date” means the date on which the Agreement is executed by the parties;

“Expert Committee” means and comprise of independent experts in the field of information technology and finance as appointed by the parties within 2 (two) weeks from Effective Date;

"Final Acceptance" means and includes successful implementation of all components of the Solution, submission of test results as per Acceptance Test Plan and SEBI shall thereafter certify to the Solution Partner in writing SEBI’s Acceptance of the Systems and warranty will apply only after such final acceptance;

“Final Destination” means specific “Location” as finalized by SEBI for the delivery & Installation of the goods or products under the RFP

“Force Majeure” means a circumstance beyond the reasonable control of a party which results in that party being unable to observe or perform on time an obligation under this RFP. These circumstances include:

(i) acts of God, lightning, earthquakes, floods, storms, explosions, fires and any natural disaster;

(ii) acts of war, acts of public enemies, terrorism, riots, civil commotion, malicious damage, sabotage and revolution;

“Go-Live Date” means the date on which SEBI first uses the System after Final Acceptance in actual production;

“Goods" or "**Products”** means all of the equipment, software including third party software, if any, supplies and consumable items that Solution Partner is required to supply, deliver, install and operationalise or provide under this RFP, including the associated documentation thereof;

"Information" includes data, text, images, sound, voice, codes, computer programmes, software and databases or micro film or computer generated micro fiche;

“Systems” means all of the products and services to be supplied, delivered, installed, integrated and made operational, together with the services to be delivered by the Solution Partner under this RFP for the purpose, as specified therein;

“Intellectual Property Rights” means any and all copyright, moral rights, trademark, patent, and other intellectual and proprietary rights, title and interests, world-wide, whether vested, contingent or future, including without limitation all economic rights and all exclusive rights to reproduce, fix, adapt, modify, translate, create derivative works from, manufacture, introduce into circulation, publish, distribute, sell, license, sublicense, transfer, rent, lease, transmit or provide access electronically, broadcast, display, enter into computer memory, or otherwise use any portion or copy, in whole or in part, in any form, directly or indirectly, or to authorize or assign others to do so;

“Implementation Period” means the period till the final user acceptance test as per the Project Plan;

“Installation” means Solution Partner’s written notification indicating that the Systems (or a specific part thereof) have been installed by the Solution Partner in accordance with the RFP requirements and the Project Plan, and are ready for Acceptance;

“Location” means the premises in India occupied by SEBI from time to time for the purposes of its operations or as otherwise notified to the Solution Partner in writing from time to time;

“Maintenance Period” is the period of 4 Years for maintenance and Support Services for the Systems under this RFP, as measured from the expiration of the 3 Years Warranty Period;

“Milestone” means the stages designated by the Solution Partner for achieving the task set out in the Project Plan;

“Party" or **"Parties”** means SEBI and the Solution Partner under the Agreement;

“Performance Bank Guarantee” means the bank guarantee to be provided by the Solution Partner to SEBI for due performance as per this RFP;

“Price" or **"Consideration”** means the price payable to the Solution Partner by SEBI under this RFP for the full and proper performance of contractual obligations;

“Project” means the installation, testing and operationalisation of the Solution to be provided by the Solution Partner in terms of this RFP;

“Project Plan” means the schedule of task to be carried out and completed by the Solution Partner on the various scheduled dates and to be duly approved by SEBI from time to time;

“Project Manager” means the full time personnel(s) designated by the Solution Partner and SEBI and who shall be single point of contact in the matter connected with the Project;

“Services” means those services associated with the supply, delivery, installation and operationalisation of the Systems;

“Software” means instructions that cause data processing systems to perform or execute specific operations;

“Source Code” means the database structures, dictionaries, definitions, program source files and any other representations necessary for the compilation, execution and subsequent maintenance of the custom and/or application software;

“Standard Software” means system and general purpose software;

(a) **"system software"** includes the operating system, communications system and network management and utility software;
(b) **"general purpose software"** includes word-processing, spreadsheet, and generic database management and application development software;

"Subcontractor" means any person or his legal representatives, his personnel to whom part of this contract has been sublet by the Solution Partner after written consent of SEBI;

“Tenure of the agreement” means a period including implementation, warranty and AMC.
"Upgrades" means revision of a software product or a system software or repair/replacement of a manufacturing hardware component like memory, hard disk, CPU as available in the Original Equipment Manufacturer (**“OEM”**) agreement of warranty and AMC;

"Updates" means bug-fixes in a software product or a system software or repair/replacements of a manufacturing hardware components like memory, hard disk, CPU as available in the OEM agreement or warranty and AMC;

“Warranty Period” is the 3 Years period specified in this RFP, following the Acceptance of the entire Solution during which the Solution Partner’s warranty obligations in respect of the supplied System are in force.

LIST OF ABBREVIATIONS/ACRONYMS

Abbreviation	**Full Form**
AMC	ANNUAL MAINTENANCE CONTRACT
CD	COMPACT DISC
CDSL	CENTRAL DEPOSITORY SERVICES LIMITED
DC	DATA CENTER
EMD	EARNEST MONEY DEPOSIT
GUI	GRAPHICAL USER INTERFACE
ITD	INFORMATION TECHNOLOGY DEPARTMENT
MSA	MASTER SERVICE AGREEMENT
NA	NOT AVAILABLE
NDA	NON DISCLOSURE AGREEMENT
NPV	NET PRESENT VALUE
OEM	ORIGINAL EQUIPMENT MANUFACTURER
PD	PEN DRIVE
POC	PROOF OF CONCEPT
POE	POWER ON ETHERNET
PR	PRIMARY SITE
RFP	REQUEST FOR PROPOSAL
SEBI	SECURITIES AND EXCHANGE BOARD OF INDIA
SI	SOLUTION INTEGRATOR
SLA	SERVICE LEVEL AGREEMENT
TCO	TOTAL COST OF OWNERSHIP
WFH	WORK FROM HOME
WLC	WIRELESS CONTROLLER

1. Request for Proposal Process

1.1. Fact Sheet

Clause Reference	**Topic**
3.3	The method of selection is Lowest Cost Based Selection.
-	RFP can be downloaded from *www.sebi.gov.in* and
1.6.2	EMD of Rs. 80 Lakhs only) in the form of Demand Draft OR Bankers Cheque OR bank guarantee in favour of "Securities and Exchange Board of India": Payable at Mumbai.
1.5	A pre-bid meeting will be held on January 14, 2021 at 11 AM, at SEBI Bhavan, Plot No. C4-A, G Block, Bandra Kurla Complex, Bandra (East) - 400051, India The name, address, and telephone numbers of the nodal officer is: Rajveer Singh Yadav Manager SEBI, SEBI Bhavan, +91-22-2644-*9519* or +91-22-4045-*9519* netup@*sebi.gov.in* All queries should be received on or before January 07, 2021, 6 PM , through email on **netup@sebi.gov.in** only.
1.6.3.q	Taxes: As applicable
1.7.3	Proposals must remain valid for120 days after the submission date, i.e., until: May 28, 2021.
1.6.3.b	Bidders must submit: • An original along with one copy in a non-editable CD/DVD/HDD/Pen Drive for technical proposal along with signed copy of this RFP in acceptance of all clauses of RFP • One original along with one copy in a non-editable CD/DVD/HDD/Pen Drive for commercial proposal. • EMD
1.7.2	The proposal submission address is: Chief General Manager – ITD *Securities and Exchange Board of India* *SEBI Bhavan,*

	Plot No. C4-A, "G Block" *Bandra Kurla Complex* *Bandra (East) - 400 051* *India*
1.7.2	Proposals must be submitted no later than the following date and time January 28, 2021, 3 PM
Tenure Of the Agreement	*Implementation Period (6 Months) +3 Years Warranty & Support + 4 Years AMC*

1.2. Request for Proposal

Sealed tenders are invited from shortlisted bidders for delivery, installation, Commissioning and maintenance of SIT-NET as detailed out in the scope of work under Section 2.2 of this RFP document. The responses from RFP will be entertained only from the shortlisted bidders of EOI process. Responses and bids from bidders other than the shortlisted ones will not be opened and will summarily be rejected.

1.3. Structure of the RFP

This RFP document for the project *SIT-NET* consists of the following:

i. General instructions for bidding process
ii. Scope of Work
iii. Bid Evaluation Process
iv. Conditions Specific to Project
v. Technical/Commercial bid and other formats (Appendix I onward)

1.4. Instructions to Bidders

1.4.1. General

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

b. All information supplied by Bidders may be treated as contractually binding on the Bidders, on successful award of the assignment by SEBI based on this RFP.

c. 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 SEBI. Any notification of preferred Bidder status by SEBI shall not give rise to any enforceable rights by the Bidder. SEBI may cancel this public procurement at any time prior to a formal written contract being executed by or on behalf of SEBI.

d. This RFP supersedes and replaces any previous public documentation & communications, and Bidders should place no reliance on such communications.
e. The RFP will be issued to the eligible shortlisted bidders. SEBI reserves the right to change the requirements. Any changes made subsequently will be communicated to all the shortlisted bidders. Hence before submitting bids, bidder must ensure that such clarifications/changes have been considered by them. SEBI will not have any responsibility in case some omission is done by any bidder.
f. Each page of the technical as well as commercial bid and any supplementary document attached, should have the signature and the seal of an authorized person. In case of electronic submission, the documents should be digitally signed.
g. All the information/documents sought through the RFP should be provided. Incomplete information/documents may lead to rejection.
h. SEBI shall not be responsible for non-receipt/non-delivery of bid documents due to any reason.
i. The response to the RFP should be in English only.
j. All prices should be quoted in Indian Rupees only.
k. Notwithstanding anything contained herein above, in case of any dispute, claim and legal action arising out of this RFP, the parties shall be subject to the jurisdiction of courts at Mumbai, Maharashtra, India only.
l. This RFP is meant only for the short-listed bidders who have responded to the EOI no. SEBI/ITD/HO/2020/07/01 dated July 08, 2020. Responses and bids from bidders other than the shortlisted ones will not be opened and will summarily be rejected.
m. All prices shall be in INR.

1.4.2. Compliant Proposals / Completeness of Response

a. Bidders are advised to study all instructions, forms, terms, requirements and other information in the RFP documents carefully. Submission of the bid shall be deemed to have been done after careful study and examination of the RFP document with full understanding of its implications.
b. Failure to comply with the requirements of this paragraph may render the Proposal non-compliant and the Proposal may be rejected. Bidders must:
    i. Include all documentation specified in this RFP;
    ii. Follow the format of this RFP and respond to each element in the order as set out in this RFP;
    iii. Comply with all requirements as set out within this RFP.

1.4.3. Code of Integrity

No official of SEBI or a bidder shall act in contravention of the codes which includes-

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

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

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

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

iv. Any financial or business transactions between the bidder and any official of SEBI related to tender or execution process of contract; which can affect the decision of SEBI directly or indirectly.

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

vi. Obstruction of any investigation or auditing of a procurement process.

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

b. Disclosure of conflict of interest.

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

In case of any reported violations, SEBI, after giving a reasonable opportunity of being heard, concludes that a bidder, as the case may be, has contravened the code of integrity, may take appropriate measures.

1.5. Pre-Bid Meeting & Clarifications

1.5.1. Pre-bid Conference

a. SEBI shall hold a pre-bid meeting with the Bidders on January 14, 2021, 11 AM at SEBI Bhavan, Plot No. C4-A, G Block, Bandra Kurla Complex, Bandra (East) - 400051, India .

b. The Bidders will have to ensure that their queries for pre-bid meeting should reach at *netup@sebi.gov.in* on or before January 07, 2021, 6 PM.

c. The queries should necessarily be submitted in the following format:

Bidder Name :					
Contact Person :					
Contact no / Email id:					
SN	**RFP Section No.**	**RFP Page No**	**RFP Clause no.**	**Existing Clause Details**	**Clarification Sought**

d. SEBI shall not be responsible for ensuring that the Bidders' queries have been received by them. Any requests for clarifications post the indicated date and time may not be entertained by SEBI.

1.5.2. Responses to Pre-Bid Queries and Issue of Corrigendum

a. The Nodal Officer notified by SEBI will endeavour to provide timely response to all queries. However, SEBI makes no representation or warranty as to the completeness or accuracy of any response made in good faith, nor does SEBI undertake to answer all the queries that have been posed by the Bidders.

b. At any time prior to the last date for receipt of bids, SEBI may, for any reason, whether at its own initiative or in response to a clarification requested by a prospective Bidder, modify the RFP Document by a corrigendum.

c. The corrigendum (if any) & clarifications to the queries from all Bidders will be emailed to all participants of the pre-bid conference.

d. Any such corrigendum shall be deemed to be incorporated into this RFP.

e. In order to provide prospective Bidders reasonable time for taking the corrigendum into account or for any other reasons at it deems fit, SEBI may, at its discretion, extend the last date for the receipt of Proposals.

1.6. Key Instructions of the Bid

1.6.1. Right to Terminate the Process

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

b. This RFP does not constitute an offer by SEBI. The Bidder's participation in this process may result SEBI selecting the Bidder to engage towards execution of the subsequent contract.

1.6.2. Earnest Money Deposit (EMD)/ Bid Security

a. Bidders[1] shall submit, along with their Proposals, an EMD of Rs. 80 Lakhs *only*), in the form of a demand draft OR Bankers Cheque OR bank guarantee (Appendix I Form 18). The payment transfer related information is as follows:

    i. Demand Draft/Banker cheque in favour of "Securities and Exchange Board of India": Payable at Mumbai.

b. EMD of all unsuccessful Bidders would be refunded by SEBI not later than 30 days of awarding of contract to the selected bidder. The EMD, for the amount mentioned above, of successful Bidder would be returned upon submission of Performance Bank Guarantee as per the format provided in Appendix VIII.

c. The EMD amount is interest free and will be refundable to the unsuccessful Bidders without any accrued interest on it.

---

[1] except for specific class of Bidders exempted under GFR

d. Proposals not accompanied with the EMD or containing EMD with infirmity (ies) (relating to the amount or validity period etc.), mentioned above, shall be summarily rejected.

e. The EMD may be forfeited in the event of:
   - A Bidder withdrawing its bid during the period of bid validity.
   - A successful Bidder fails to sign the subsequent contract in accordance with this RFP.
   - The Bidder being found to have indulged in any suppression of facts, furnishing of fraudulent statement, misconduct, or other dishonest or other ethically improper activity, in relation to this RFP.
   - A Proposal contains deviations, conditional offers and partial offers.

1.6.3. Submission of Proposals/ Guidelines for Bidders

a. The Bidders should ensure that all assumptions/clarifications required are clarified before the conclusion of pre-bid meeting. Any bids with words/phrases such as (but not limited to) “assumption”, “it is understood that”, “conditional offer” may be subjected to rejection at any stage of evaluation.

b. Bidders should submit their responses as per the formats given in this RFP in the following manner:
   i. Technical Proposal - (1 original + 1 CD/DVD/HDD/USB Drive) in one envelope
   ii. Commercial Proposal - (1 original + 1 CD/DVD/HDD/USB Drive) in second envelope
   iii. EMD in third envelope

   In case of electronic submission, the documents should be digitally signed.

c. The Bidder’s Proposal in response to technical and commercial evaluation (as mentioned in previous paragraph) should be covered in separate sealed envelopes super scribing "Technical Proposal for SEBI Enterprise-wide Integrated IT Network Infrastructure (SIT-NET) " and “Commercial Proposal for SEBI Enterprise-wide Integrated IT Network Infrastructure (SIT-NET)” respectively.

d. Please note that prices should not be indicated in the technical proposal but should only be indicated in the commercial proposal. However, a masked bill of material masking the price information be provided along with the technical proposal.

e. The one envelope containing copies of technical Proposal and commercial Proposal should be put in another single sealed envelope clearly marked “Response to RFP for SEBI Enterprise-wide Integrated IT Network Infrastructure (SIT-NET) - SEBI /ITD/HO/2020/12/02 and the wordings “DO NOT OPEN BEFORE January 28, 2021.

f. The outer envelope thus prepared should also indicate clearly the name, address, telephone number and E-mail ID of the Bidder to enable the Bid to be returned unopened in case it is found to be received after the time and date of Proposal submission prescribed herein.

g. All the pages of the Proposal must be sequentially numbered and must contain the list of contents with page numbers. Any deficiency in the documentation may result in the rejection of the Bidder’s Proposal.
h. The original Proposal shall be prepared in indelible ink. It shall contain no interlineations or overwriting, except as necessary to correct errors made by the Bidder itself. Any such corrections must be initialled by the authorized signatory of the Bidder.
i. All pages of the bid shall be initialled and stamped by the authorized signatory of the Bidder.
j. The Bidder must submit a certificate of undertaking on its official letter-head duly signed by its authorized signatory confirming the acceptance of all the terms & conditions contained in and spread throughout this Bid Document.
k. Decision as to any arithmetical error, manifest or otherwise in the response to Bid Document shall be decided at the sole discretion of SEBI and shall be binding on the Bidder. Any decision of SEBI in this regard shall be final, conclusive and binding on the Bidder.
l. Bidder must ensure that the information furnished by him in respective CD/DVD/HDD/USB Drive is identical to that submitted by him in the original paper bid document. In case of any discrepancy observed by SEBI in the contents of the CD/DVD/HDD/USB Drive and original paper bid documents, the information furnished on original paper bid document will prevail over the soft copy.
m. Bidder should be a legal entity and financially solvent. Bidder must warrant that no legal action is pending against them in any legal jurisdiction which affects its ability to deliver the RFP requirements.
n. SEBI reserves the right to re-issue/re-commence the entire bid process in case of any anomaly, irregularity or discrepancy in regard thereof. Any decision of SEBI in this regard shall be final, conclusive and binding on the Bidder.
o. Modification to the RFP, if any, will be made available as an addendum on SEBI’s website/will be emailed to bidder.
p. Successful Bidder would sign along with the Contract Form and other forms contained in the Bid Document, the Non-Disclosure Agreement (NDA) with SEBI, to protect any shared sensitive information/data.
q. Prices quoted should be exclusive of GST. The taxes will be payable at applicable rates at the time of raising the invoice.
r. Prices quoted must be firm till the completion of the contract including Warranty & Support, and AMC period.
s. The Bid Price quoted is to be written in words as well as figures and in case of discrepancies between the price written in words and price written in figures, the price written in words shall be considered to be correct.
t. SEBI’s decision in respect to evaluation methodology and short-listing Bidders will be final and no claims whatsoever in this respect will be entertained.
u. The bidders should have back to back support and service agreements with OEM's for all the components of SIT-NET where applicable during Warranty & Support, and AMC period. A letter from the OEM should be submitted in this regard as part

of response to RFP.

v. 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 returned unopened.

w. The bids shall be submitted strictly in accordance to clause 1.7.2. Submission through any other means such as e-mail etc. shall not be considered. No correspondence will be entertained on this matter.

x. SEBI shall not be responsible for any postal delay or non-receipt/ non-delivery of the documents. No further correspondence on the subject will be entertained.

y. The bidder understands that if at any stage, information provided by the bidder /OEMs is found to be inaccurate, SEBI may, at its discretion, disqualify the bidder and/or OEMs.

z. The bidder will provide demonstration of products, arrange lab visit, site visit or POC if required by SEBI during technical evaluation of the product to cross check functionalities. The bidder/OEMs will ensure the availability of necessary environment in all aspects for SEBI's verification process.

aa. The bidder understands that SEBI retains the right to ask to demonstrate certain scenarios, details of which will not be provided in advance, the right to reject the offer at any stage of the process without assigning any reasons and SEBI will not be liable to pay any costs incurred by the vendor during technical verification process.

bb. The bidder understands that the Intellectual Property Rights for all the solutions designed for SIT-NET will rest solely with SEBI and no claims will be made in this regard by the bidder and OEMs.

cc. The bidder accepts to follow all the clauses, terms and conditions as set in the RFP document.

dd. SEBI reserves the right to modify and amend any of the above-stipulated condition/criterion depending upon project priorities vis-à-vis urgent commitments.

ee. The Bidder shall also submit INTEGRITY PACT along with technical proposal (**Appendix I – Form 2**) duly signed by the Bidder on each page and witnessed by two persons. The agreement shall be stamped as applicable in the State where it is executed. Bid submitted without PRE-CONTRACT INTEGRITY PACT, as per the format provided in the RFP, shall not be considered.

1.6.4. Bidder's Authorized Signatory

A Proposal should be accompanied by an appropriate board resolution or power of attorney in the name of an authorized signatory of the Bidder stating that (s)he is authorized to execute documents and to undertake any activity associated with the Bidder's Proposal.

1.7. Preparation and Submission of Proposals

1.7.1. Proposal Preparation Costs

The Bidder shall be responsible for all costs incurred in connection with participation in the RFP process, including, but not limited to, costs incurred in conduct of informative and other diligence activities, participation in meetings/discussions/presentations, preparation of proposal, in providing any additional information required by SEBI to facilitate the evaluation process, and in negotiating a definitive contract or all such activities related to the bid process. SEBI will in no event be responsible or liable for those costs, regardless of the conduct or outcome of the bidding process.

1.7.2. Venue & Deadline for Submission of Proposals

Proposals, in its complete form in all respects as specified in the RFP, must be submitted to SEBI at the address specified below on or before January 28, 2021, 3 PM.

Chief General Manager – ITD
Securities and Exchange Board of India
SEBI Bhavan,
Plot No. C4-A, "G Block"
Bandra Kurla Complex
Bandra (East) - 400 051
India

1.7.3. Proposal Validity

The offer submitted by the Bidders should be valid for minimum period of 120 days from the date of submission of the Proposal.

1.7.4. Proposal Opening

The Proposals submitted before deadline will be opened at January 28, 2021, 3:30 PM by the Bid Opening Committee authorized by SEBI, in the presence of the Bidder's representatives who may be present at the time of opening.

The representatives of the Bidders are advised to carry an identity card or a letter of authority from the Bidding entity to identify their bona fide for attending the opening of the Proposal.

1.7.5. Proposal Evaluation

a. Initial Proposal scrutiny will be held to confirm that Proposals do not suffer from the infirmities detailed below. Proposals will be treated as non-responsive, if a Proposal is found to have been:

- submitted in manner not conforming with the manner specified in the RFP document
- Submitted without appropriate EMD as prescribed herein
- received without the appropriate power of attorney or letter of authority
- containing subjective/incomplete information
- submitted without the documents requested in the checklist
- non-compliant with any of the clauses stipulated in the RFP
- having less than the prescribed validity period

The EMD of all non-responsive bids shall be returned to the bidders.

b. All responsive Bids will be considered for further processing as below. SEBI will prepare a list of responsive Bidders, who comply with all the Terms and Conditions of the Tender. All eligible bids will be considered for further evaluation by a Committee according to the Evaluation process defined in this RFP document. The decision of the Committee will be binding, final and conclusive in this regard.

1.8. Terms and Conditions of this RFP

1.8.1. Award Criteria

SEBI will award the Contract to the L1 Bidder as per the process outlined in Section 3.

1.8.2. Information Provided

The Request for Proposal document contains statements derived from information that is believed to be relevant at the date but does not purport to provide all of the information that may be necessary or desirable to enable an intending contracting party to determine whether or not to enter into a contract or agreement with SEBI. Neither SEBI nor any of its employees, contractors, and advisors gives any representation or warranty, expressed or implied, as to the accuracy or completeness of any information or statement given or made in this document. Neither SEBI nor any of its employees, contractors, and advisors has carried out or will carry out an independent audit or verification exercise in relation to the contents of any part of the document.

1.8.3. Errors and Omissions

Each Recipient should notify SEBI of any error, omission, or discrepancy found in this RFP document, if any.

1.8.4. Eligible Goods

The Bidder shall demonstrate their right to sell, license or distribute the software proposed in response to this RFP. In case of contractual arrangements, it will be the sole responsibility of the Bidder to make all necessary contractual arrangements across all components of the solution. Bidders shall also be responsible for obtaining all necessary export permits, if applicable, for the products and services to be supplied.

1.8.5. Partnership / Collaboration

If the Bidder is working on a joint venture/collaboration/consortium, the details of the same along with the responsibilities of the partners shall be mentioned. However, the Bidder shall submit an undertaking letter jointly executed by him/her and his/her collaborator/associate for the satisfactory performance of the project along with the Technical Bid. If the Bidder is offering solutions/products from other Bidders/principals, in response to this RFP, it shall detail the responsibilities of the parties involved and also submit a letter of undertaking from the parties mentioning their consent and assurance for satisfactory performance of the project along with the Technical Bid. The Bidder shall submit a certificate, duly signed by the authorized official, along with the Technical Bid that change in ownership is not anticipated in the proposed period of contract defined during the 'tenure of the agreement'. If such a change is anticipated, the scope and effect thereof shall be defined.

1.8.6. Format and Signing of Bid

The original Bids shall be typed or printed in a clear typeface. Each tender/ RFP response shall be made in the legal name of the Bidder and shall be signed by the Bidder or a person duly authorized to sign on behalf of the Bidder. The Bidder's authorized signatory shall authenticate by sign and seal, each page of the Bid including brochures/pamphlet/write-up etc. Bids with erasure/over writing/cutting are liable to be rejected. If required, the corrections can be made by scoring out entries and writing afresh. The authorized signatory shall authenticate each correction. Wherever certification/undertaking is submitted, the Bidder shall affix signature with name, title/designation and seal in addition to page-wise authentication. The Bidder's signature shall be deemed to imply unqualified acceptance of the Terms and Conditions of RFP.

1.8.7. Notification of Award

The notification of award, subject to contract/ agreement, will be communicated in writing at the address supplied by the Bidder in the tender/RFP response. Any change of address of the Bidder, should therefore be promptly notified to:

Chief General Manager – ITD
Securities and Exchange Board of India
SEBI Bhavan,
Plot No. C4-A, "G Block"
Bandra Kurla Complex
Bandra (East) - 400 051
India

1.8.8. Signing of Agreement

The parties shall enter into a contract as per appendix ix “Draft Master Service Agreement”, incorporating all clauses, pre-bid clarifications and the proposal of the Bidder, between SEBI and the successful Bidder.

1.8.9. Governing Law and Disputes

The Bid and the Contract/ Agreement resulting there from with the selected Bidder shall be governed in accordance with the Laws of India and will be subject to the exclusive jurisdiction of Courts at Mumbai irrespective of the place of the cause of action and rights and liabilities of the Parties hereto.

All disputes or differences whatsoever arising between SEBI and the Bidders out of meaning and operation or effect of this RFP Document or breach thereof, shall be settled amicably. If, however, the parties, as above, are not able to resolve them amicably, the same shall be settled by arbitration in accordance with the applicable Indian Laws, and the award made in pursuance thereof shall be binding on the parties, as above. Any appeal will be subject to the exclusive jurisdiction of the courts at Mumbai, India. In such instances, the Bidder shall continue work under the Contract/Agreement during the arbitration proceedings unless otherwise directed in writing by SEBI or unless the matter is such that the work cannot possibly be continued until the decision of the Arbitrator or of the umpire, as the case may be, is obtained. The venue of the arbitration shall be Mumbai, India.

1.8.10. Content and Form of Responses

In order to facilitate evaluation and comparison of bid responses, Bidders must submit their response in the format prescribed herein, failing which their Bid may be eliminated as not being responsive to this RFP document. The bid contains two part viz. Part A - Technical Bid and Part B -Commercial Bid. If the Bidder wants to include any additional information other than those indicated hereunder, the same may be added at the end of Part A by inserting separate sheets without altering SEBI’s Technical Bid format.

1.8.11. Consortium /Teaming Arrangement

In case of consortium bid with Bidder, the Bidder must submit a letter from members of the consortium confirming their participation in the bid and agreeing to the conditions of the RFP and agreement to support the project implementation and subsequent Warranty & Support, and AMC period for the project. The letter should clearly specify the Bidder and members of the consortium with their roles, responsibility and authority clearly mentioned. Any change or divergence in the roles or responsibility after the award of co44ntract by the Bidder shall be taken, as non-performance of the contract and SEBI will have the right to terminate the contract at its discretion, which will result in the forfeiture of EMD. The actual teaming agreement must be provided to SEBI by the time of Commercial Bid Opening. In case there is any divergence from the conditions defined in the RFP, SEBI reserves the right to reject the bid and forfeiture of the EMD.

1.8.12. Subcontracting

In case, the Bidder wishes to delegate, assign or otherwise arrange for the provision of all or part of the Services to be performed by the agent, contractor, supplier, or vendor of supplier, the Bidder shall explicitly mention the same in its proposal. Bidder is required to submit relevant details of proposed subcontractor as mentioned in the section 3.2.1.

Unless and otherwise specified in the proposal, any form of subcontracting shall not be allowed.

Further, the Bidder should ensure that the extant labour laws are being adhered by the subcontractor.

The Bidder shall remain responsible for obligations, Services and functions performed by subcontractors to the same extent as if such obligations, Services and functions were performed by the Bidder's employees and for purposes of this project, such work shall be deemed work performed by the Bidder. For the avoidance of doubt, Bidder expressly acknowledges and agrees that its obligations under this clause do not relieve or otherwise diminish Bidder's confidentiality, liability and indemnification obligations under this RFP in the event a subcontractor breaches the terms of Bidder's agreement with the subcontractor as contemplated by this clause.

1.8.13. Workmen Safety and Insurance

The Bidder shall alone be fully responsible for safety and security and insurance or life insurance of their personnel (including those of subcontractor) who is working on the project. The Bidder at SEBI's request, shall provide evidence to SEBI showing that such insurance has been taken out and maintained and that the current premiums have been paid. SEBI shall not be liable for any compensation in case of any fatal injury/ death caused to or by any man power while performing/discharging their duties/for inspection or otherwise. The Bidder shall adhere to all the extant labour laws.

1.8.14. Technological Upgrade

Further, the bidder should upgrade equipment with the latest software versions as part of technological up-gradation i.e., equipment OS up-gradation/application up-gradation etc., and timely application of patches (specially security patches), as and when required, without any additional cost so as to deliver the SLA's specified during the contract period. Bidder will sign up back-to-back contract with the OEM for regular upgrades and updates.

There are instances where to perform such updates/upgrades, it is required to change custom developed application or migrate data from older version to newer version. These will be undertaken through Change Requests Management Framework.

Any required hardware upgrades undertaken by SEBI, version/ software upgrades/updates, patch management etc. will be supported by Bidder for the entire duration of Agreement at no extra cost to SEBI. As part of warranty and support, and subsequent AMC it is expected that all software updates, upgrades, bug fixes etc. would be supplied and supported by bidder to SEBI at no additional cost.

Any hardware upgrade undertaken by SEBI during the tenure of project will not impact the terms of warranty and support.

1.8.15. Right to Accept Any Proposal and To Reject Any or All Proposal(s)

SEBI reserves the right to accept or reject any proposal, and to annul the tendering process/ Public procurement process and reject all proposals at any time prior to award of contract, without thereby incurring any liability to the affected Bidder or Bidders or any obligation to inform the affected Bidder or Bidders of the grounds for SEBI action.

1.8.16. Failure to Agree with the Terms and Conditions of the RFP

Failure of the successful Bidder to agree with the Draft MSA and Terms & Conditions of the RFP shall constitute enough grounds for the annulment of the award, in which event SEBI may award the contract to the next best value Bidder or call for new proposals from the interested Bidders.
In such a case, SEBI shall invoke the PBG/forfeit EMD of the successful Bidder.

1.8.17. Payment Process

i. The Bidder’s requests for payment shall be made to SEBI in writing accompanied by Original Invoice detailing the systems, software delivered, installed and accepted by SEBI.

ii. The payment after deducting applicable TDS, wherever applicable as may be specified by Government in this behalf, will be released by SEBI. All payments will be made only by electronic transfer of funds either by NEFT or RTGS. The Bidder therefore has to furnish SEBI account number to where the funds have to be transferred for effecting payments.

iii. Payments as per the schedule given in Section 4.3 will be released only on acceptance of the order and on signing the agreement/contract by the selected bidder and also on submission of performance bank guarantee in the specified format.

iv. Payment will be processed only after submission of necessary documents like delivery challan, Installation/commissioning report, SLA reports, etc. duly signed by authorized SEBI person and road permit receipt (if any), accompanied by the Invoice.

v. The bidder must accept the payment terms and conditions proposed by SEBI. Any deviation from the proposed payment terms would not be accepted. SEBI shall have the right to withhold any payment due to the bidder, in case of delays or defaults on the part of the bidder.

vi. The Invoices will be raised as per the Milestones mentioned in Section 4.3. It would be the responsibility of the bidder to ensure submission of the invoices, for the setting up of SIT-NET.

vii. The price quoted by the bidder should not change due to exchange rate fluctuations, inflation, market conditions, and increase in custom duty. Prices quoted must be firm till the completion of the contract.

1.8.18. Restrictions under Rule 144 (xi) of the General Financial Rules (GFRs), 2017

i. Any bidder from a country which shares a land border with India will be eligible to bid in this tender only if the bidder is registered with the Competent Authority.

ii. "Bidder" in para 1.8.18 i. above (including the term 'tenderer', 'consultant' or 'service provider' in certain contexts) means any person or firm or company, including any member of a consortium or joint venture (that is an association of several persons, or firms or companies), every artificial juridical person not falling in any of the descriptions of bidders stated herein before, including any agency branch or office controlled by such person, participating in a procurement process.

iii. "Bidder from a country which shares a land border with India" for the purpose of this Order means: –

   a. An entity incorporated, established or registered in such a country; or
   b. A subsidiary of an entity incorporated, established or registered in such a country; or
   c. An entity substantially controlled through entities incorporated, established or registered in such a country; or
   d. An entity whose beneficial owner is situated in such a country; or
   e. An Indian (or other) agent of such an entity; or
   f. A natural person who is a citizen of such a country; or
   g. A consortium or joint venture where any member of the consortium or joint venture falls under any of the above

iv. The beneficial owner for the purpose of (iii) above will be as under:

1) In case of a company or Limited Liability Partnership, the beneficial owner is the natural person(s), who, whether acting alone or together, or through one or more juridical person, has a controlling ownership interest or who exercises control through other means.

   Explanation-

   a. “Controlling ownership interest” means ownership of or entitlement to more than twenty-five per cent. of shares or capital or profits of the company;
   b. “Control” shall include the right to appoint majority of the directors or to control the management or policy decisions including by virtue of their shareholding or management rights or shareholders agreements or voting agreements;

2) In case of a partnership firm, the beneficial owner is the natural person(s) who, whether acting alone or together, or through one or more juridical person, has ownership of entitlement to more than fifteen percent of capital or profits of the partnership;

3) In case of an unincorporated association or body of individuals, the beneficial owner is the natural person(s), who, whether acting alone or together, or through one or more juridical person, has ownership of or entitlement to more than fifteen percent of the property or capital or profits of such association or body of individuals ;

4) Where no natural person is identified under 1) or 2) or 3) above, the beneficial owner is the relevant natural person who holds the position of senior managing official;

5) In case of a trust, the identification of beneficial owner(s) shall include identification of the author of the trust, the trustee, the beneficiaries with fifteen percent or more interest in the trust and any other natural person exercising ultimate effective control over the trust through a chain of control or ownership.

v. An Agent is a person employed to do any act for another, or to represent another in dealings with third person.

vi. The successful bidder shall not be allowed to sub-contract works to any contractor from a country which shares a land border with India unless such contractor is registered with the Competent Authority.

1.9. Fraud and Corrupt Practices

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

b. Without prejudice to the rights of SEBI under Clause above and the rights and remedies which SEBI may have under the Agreement, if a Bidder or Systems Integrator Agency, as the case may be, is found by the Authority to have directly or indirectly or through an agent, engaged or indulged in any corrupt practice, fraudulent practice, coercive practice, undesirable practice or restrictive practice during the Selection Process, or after the execution of the Agreement, such Bidder or Systems Integrator Agency shall not be eligible to participate in any tender or RFP issued by SEBI during a period of 2 (two) years from the date such Bidder or Systems Integrator Agency, as the case may be, is found by SEBI to have directly or through an agent, engaged or indulged in any corrupt practice, fraudulent practice, coercive practice, undesirable practice or restrictive practice, as the case may be.

c. For the purposes of this Section, the following terms shall have the meaning hereinafter respectively assigned to them:

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

ii. “fraudulent practice” means a misrepresentation or omission of facts or disclosure of incomplete facts, in order to influence the Selection Process;

iii. “coercive practice” means impairing or harming or threatening to impair or harm, directly or indirectly, any persons or property to influence any person’s participation or action in the Selection Process;

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

v. “restrictive practice” means forming a cartel or arriving at any understanding or arrangement among Bidders with the objective of restricting or manipulating a full and fair competition in the Selection Process.

vi. **Independent External Monitors (IEMs)**: The details of Independent External Monitors (IEMs) who will monitor the tender process and the execution of the contract for compliance with the principles are mentioned below:

Sr. No.	Names	Email ID
1	Shri Ajai Kumar	ajai.kumar3@gmail.com
2	Smt. Rajni Sekhri Sibal	rajnisekhrisibal@gmail.com

2. Scope of Work and Deliverable

2.1. Background Information

2.1.1. About SEBI

Securities and Exchange Board of India (hereinafter referred as SEBI) was established under an Act of Parliament, to protect the interests of investors in securities and to promote the development of, and to regulate, the securities market and for matters connected therewith or incidental thereto. Detailed information on the functions of SEBI is provided on the website, www.sebi.gov.in.

2.1.2. Project Background

SEBI has upgraded its Network Infrastructure in 2013-14 which is now due for a revamp. Accordingly, SEBI proposes to upgrade its current IT Network Infrastructure comprising of Network Devices, IP Telephony, Wireless Solution etc. across its Head office[2], Regional offices and Local offices. A seamless network solution is expected to be designed and implemented with the latest available technologies ensuring a reliable, secured, integrated, always available and scalable solution with no single point of failure.

2.1.3. Envisaged Benefits

The following objectives/benefits are to be derived from the SIT-NET includes but not limited to –

a) **Sizing, Accessibility and Augmentation**: The proposed solution should be scalable taking into account the growth of man power and IT resources in the organization. The emerging MAN-WAN topology and access from home solution have to be incorporated to ensure wider accessibility of IT infrastructure resources in SEBI. This would require appropriate solutioning both at node as well as leaf levels. It is envisaged that the proposed solution would offer an integrated access to SEBI users with unified AD, DNS, DHCP. Additionally, SEBI will provide IT networking features like VPN, BYOD, IP phones, Wi-Fi access to all the employees with functionality based upon their grade including outsourced staff. The proposed solution would be agnostic to the underlying hardware, which would enable seamless upgradation when required.

b) **Integrated Secured Operations**: The solution would support the latest network and security technologies and have tight integration with SEBI's NOC-SOC technologies already implemented in SEBI. The proposed

---

[2] Head Office – SEBI Bhavan, SEBI Bhavan 2, NCL and Mittal Court office.

solution should also implement Zero Trust Model and ensure segregation of North-South and East-West traffic.

c) **Support and Manageability improvement:** The size of SEBI IT Network Infrastructure reach has grown and so is the dependence on the same for day to day functioning of SEBI. Through mandatory compliance to the accepted SLA, near zero down-time is envisaged at all levels. Based on SEBI’s requirements of managing a large network infrastructure through a centralized control and making the network infrastructure available at all locations, usability of emerging and cost effective technologies like Software Defined Network (SDN) and Network Access Control (NAC) needs to be provided. The solution would facilitate Patch Management at all levels thus ensuring updated versions of applications and OS across the SEBI infrastructure.

d) **Integrated Video conferencing solution at SEBI:** Since video conferencing solution is integrated with network devices, hence it is proposed to leverage the emerging technology solutions to build an integrated video conferencing solution across all offices of SEBI.

2.2. Scope of work

a) SEBI proposes to appoint a Solution Integrator (henceforth referred as Bidder) to implement and manage SEBI Enterprise-wide Integrated IT Network Infrastructure (henceforth referred as SIT-NET) with following solutions/technologies including but not limited to[3]

   i. Network Devices
   ii. IP Telephony
   iii. Wi-Fi
   iv. Software Defined Network (SDN)
   v. Network Access Control (NAC)
   vi. AD, DNS, DHCP etc.
   vii. Network Security solution
   viii. Solution for Virtual Private Network (VPN)
   ix. Video conferencing solution
   x. Patch Management solution

Note 1: Bidders are required to submit the proposal for <u>all</u> the above mentioned (2.2.a) solutions. Proposal not including any of the above solutions will be termed Deficient and will not be evaluated.

Note 2: Bidders are required to mention unit prices for all the items made under this proposal. Unit price will remain fixed during the entire duration of the agreement and SEBI reserves the right to procure the additional items at same unit price. (Refer clause 6 Appendix II: Financial Bid Templates)

b) The scope of work includes Supply, Installation, Testing, Commissioning, DR-BCP, Maintenance (3 years Warranty support and 4 years post warranty maintenance), Training and FMS Support.

c) **AMC for the existing Network Set up**:

   i. Bidders have to propose the AMC for the current (Existing) Network Project. This would be on Best Effort basis and would only be required for the implementation period (of the proposed SIT-NET solution). Bidder would be required to maintain requisite SLA levels during the said AMC period. The Bill of Material (BOM) for AMC is attached at Appendix XIII.

   ii. Bidders have to also propose AMC support for the complete project duration for the network devices as enclosed in the Appendix XIV.

---

[3] #Clause "but not limited to" mentioned in this RFP is to illustrate minimum list of components of solution that may be required to meet the desired objective of the project. Bidders are guided by the illustrative examples and may choose to add more components to deliver the desired solution.

d) **Buyback of equipment after AMC**: Bidders are required to buyback the existing network infrastructure devices (Router, Switches, Firewall, Wi-Fi Controller, IP Phone infrastructure, Servers, Access Points, etc.) after the implementation of the proposed SIT-NET infrastructure. Detailed existing inventory is provided at Appendix XIII. Bidders are also required to collect all the buyback items from the respective SEBI offices at their own cost as is where is basis after erasing or formatting the existing configuration or backup data in the mentioned network devices considered for buyback. Floor value for buyback is Rs. **36,55,000/- (Thirty-Six Lakhs Fifty-Five Thousand Rupees only).**

Note 3: Bidders have to mandatorily quote for buyback failing which their bids will not be considered for evaluation. Buyback amount will be deducted from Total cost quoted by the bidder before computation of NPV to arrive at L1 bidder.

e) **AMC of Passive Network components:**

The bidder has to provide AMC for the passive network components (Existing as well as proposed components as part of this RFP) for the complete duration of the project (Refer list of items in clause 6.2. Form 2: Detailed Technical BOM with List of Products, Solutions, Services and Licenses).

i. Supply, installation and maintenance of networking, cabling and IT infrastructure related components like racks, patch panels, sockets, I/O ports, connectors etc.

ii. Cabling between various regions of the office like hub rooms, server rooms, UPS room, cabins, workstations etc. The work also includes providing connectivity for Wi-Fi access points, at common areas like reception, usher area, entry / exit gates etc. and for essential services like BMS room, attendance system, access control, inward / outward mailing desk etc.

f) **NOC & SOC Integration:** Bidder is required to integrate all required infrastructure with SEBI’s NOC & SOC as applicable. Bidder may propose a detailed strategy for the same.

1. Bidder is responsible for doing necessary configurations for log forwarding and API/syslog integration of all the devices supplied under the project with SIEM/NMS.
2. Bidder is responsible for integration of the proposed solutions with SEBI’s Privileged Identity Management (PIM) solution.
3. Bidder is responsible for doing necessary configurations for integrating all the devices supplied under the project with existing PIM solution.

4. Bidder is responsible for doing necessary configurations carrying out any firewall configuration changes for deploying or integrating all the devices supplied under the project.
5. Detailed list of technologies to be integrated with NOC SOC is enclosed at appendix XII.

g) **Back Up:** Bidder is required to formulate appropriate backup policy and implement the same integrating with existing backup solution of SEBI. Details of Backup solution is provided at appendix XV.

h) **Training:** Bidder is required to provide training comprising of technical and hands-on on the proposed technology for 5 IT professionals. No training scheduled outside SEBI should exceed 1 (one) week (out of office) at a stretch.

The proposal should clearly articulate following key features as detailed below:

i) **The detailed scope of work includes Supply, Installation, Testing, Commissioning, DR-BCP, Maintenance (3 years Warranty support and 4 years post warranty maintenance), Training and Support. These activities may include but not limited to the following:**

Sr. No.	Scope of Work	Reference clause
1	Overall SIT-NET architecture	2.2.1
2	Capacity and Sizing	2.2.2
3	Project Management, Implementation Methodology and Timeline	2.2.4
4	Business Continuity and Disaster Recovery	2.2.5
5	Network and Security	2.2.6
6	Performance Monitoring and MIS Reports	2.2.7
7	Standards: Compatibility and Interoperability	2.2.8
8	Maintenance and Support	2.2.9
9	Versions, Upgrades and Updates	2.2.10
10	Licenses	2.2.11
11	Risk Assessment, Mitigation and Audit	2.2.13
12	Migration Plan	2.2.14

j) **Heat map of Scope of work and proposed Technologies:**

Heat map of Scope of work vs. Proposed Technologies										
Scope of Work/Proposed Technologies	**Network Devices**	**IP Telephony**	**Wi-Fi**	**Software Defined Network (SDN)**	**Network Access Control (NAC)**	**AD, DNS, DHCP etc.**	**Network Security solution**	**Virtual Private Network (VPN)**	**Video conferencing solution**	**Patch Management solution**

Overall SIT-NET architecture	▨	▨	▨	■	■	▨	■	▨	▨	▨
Capacity and Sizing	▨	■	▨	▨	▨	■	▨	■	▨	▨
Project Management, Implementation Methodology and Timeline	▨	■	▨	■	■	■	■	■	▨	▨
Business Continuity and Disaster Recovery		▨		▨		▨		▨		
Network and Security	▨	■	■	▨	■	■	■	■	▨	▨
Performance Monitoring and MIS Reports	▨	■	■	■	■	■	▨	■	▨	▨
Standards: Compatibility and Interoperability	▨	▨	■	▨	■	▨	■	■	■	▨
Maintenance and Support	▨	■	▨	▨	▨	■	▨	▨	▨	■
Versions, Upgrades and Updates	▨	▨	▨	▨	▨	▨	▨	▨	▨	■
Licenses	▨	▨	▨	▨	▨	▨	▨	▨	▨	■
Risk Assessment, Mitigation and Audit	▨	▨	■	■	▨	▨	■	■	▨	▨
Migration Plan	▨	▨				▨	▨	▨		
High Availability	▨	▨	▨	▨	▨	▨	▨			
Local Survivability		▨	▨			▨	▨		▨	

2.2.1. SIT-NET architecture:

a) The Bidder shall be responsible for design and provisioning of required IT infrastructure, underlying system software and services for deploying and hosting various applications in SIT-NET including DR site.

b) The Bidder will examine SEBI's enterprise-wide IT Network landscape that needs to be deployed on SIT-NET. This activity will enable the Bidder to gauge the required workloads criticality, complexity and the network connectivity.

c) SEBI expects that the proposed solution architecture should be optimised in terms of cooling, power, and space (number of racks) requirements. Bidder is expected to supply racks of same dimensions (**42 RU only**) as already existing in SEBI's data centre in SEBI Bhavan 2.

d) The high level view of SEBI’s current IT Network Infrastructure is attached at Appendix III (Present IT Set up of SEBI).

e) The bidders are required to integrate the proposed solution with SEBI’s other existing applications/solutions.

f) The bidders are required to change the architecture and configuration of the devices, servers etc. as and when required to meet the security guidelines, standards etc. during the entire contract period.

g) The solution shall provide NTP server time synchronization. All items delivered as part of solution should support NTP protocol. The bidders have to configure and sync timings of all the servers and devices delivered by them.

h) The solution shall support SNMP v3 for monitoring.

i) The proposed solution must integrate with SEBI’s existing SMS Gateway facility. Self Service portal for user’s password reset and other functionalities to users using MFA and secret question.

j) The proposed solution must not have any "Single point of failure" in network traffic flow and devices. Further the failure of one or more components of the solution should not affect the organizational network’s functionality. While every effort is made in RFP to ensure that no single point of failure of critical devices in network architecture, Bidders are required to identify any specific point of failure in their architecture & provide a suitable remediation. Where required, the solution should be configured in HA mode. Mandatory list of components under HA is as follows:

Table 1: HA Components

List of HA Components				
Sr. No.	**Location**	**City**	**Devices/Technologies**	**Deployment mode**
1.	SEBI Bhavan 1	Mumbai	Internal Firewall	High availability
2.	SEBI Bhavan 1	Mumbai	External Firewall	High availability
3.	SEBI Bhavan 1	Mumbai	Wi-Fi	High availability
4.	SEBI Bhavan 1	Mumbai	Server Farm Switch	High availability
5.	SEBI Bhavan 1	Mumbai	Router (Voice Gateway)	High availability

6.	SEBI Bhavan 1	Mumbai	AD/DNS/DHCP Server	High availability
7.	SEBI Bhavan 1	Mumbai	Voice Servers	High availability
8.	SEBI Bhavan 1	Mumbai	Load Balancer	High availability
9.	SEBI Bhavan 1	Mumbai	NAC	High availability
10.	SEBI Bhavan 1	Mumbai	SDN	High availability
11.	SEBI Bhavan 2	Mumbai	Internal Firewall	High availability
12.	SEBI Bhavan 2	Mumbai	External Firewall	High availability
13.	SEBI Bhavan 2	Mumbai	Core Switch	High availability
14.	SEBI Bhavan 2	Mumbai	Server Farm Switch	High availability
15.	SEBI Bhavan 2	Mumbai	Router (Voice Gateway)	High availability
16.	SEBI Bhavan 2	Mumbai	Link Load Balancer	High availability
17.	DR-Chennai	Chennai	Internal Firewall	High availability
18.	DR-Chennai	Chennai	External Firewall	High availability
19.	DR-Chennai	Chennai	AD/DNS/DHCP Server	High availability

2.2.2. Capacity and Sizing:

The Bidder will be responsible for adequately sizing the necessary Hardware and Software capacity, Count of Network devices and functionality etc., building the redundancy into the architecture and load balancing to meet the service level requirements mentioned in the RFP. The solution should be scalable and standards based and should be agnostic to the underlying hardware. **Bidders are required to mention the unit of scalability and ensure that unit price is identifiable in bill of material.** Indicative count of existing **users** using various systems, applications of SEBI is given in the appendix V.

2.2.3. Proposed Network connectivity:

If requested, SEBI’s understanding of the proposed network solution will be shared in the form of a diagram to the requesting bidder.

2.2.4. Project Management, Implementation Methodology and Timeline:

SEBI estimates to complete the implementation of SIT-NET project in 6 months. However, bidder may propose agile implementation to shorten the implementation period. Bidder may propose a suitable implementation schedule providing early visibility within 4 months of signing of the agreement. Refer to clause 2.4 and 4.2.

2.2.5. Business Continuity and Disaster Recovery Solution:

a) Business continuity plan & Disaster recovery solution

The solution should be architected to run from primary data centre. The solution should have DC and DR failover, so that if DC fails, the network and security operation should be continued from DR site. In the event of a data centre failure, there should be provision to shift traffic to the DR site. The RTO and RPO envisaged for the DR plan for each of the technology are as follows:

Table 2: Solution wise RPO-RTO requirement

Sr. No.	Technology	RPO	RTO
1	Network Devices	Not Applicable	Not Applicable
2	IP Telephony	5 Min.	10 Min.
3	Wi-Fi	Not Applicable	Not Applicable
4	Software Defined Network (SDN)	5 Min.	10 Min.
5	Network Access Control (NAC)	Not Applicable	Not Applicable
6	AD, DNS, DHCP etc.	Not Applicable	Not Applicable
7	Network Security solution	Not Applicable	Not Applicable
8	Solution for Virtual Private Network (VPN)	5 Min.	10 Min.
9	Video conferencing solution	Not Applicable	Not Applicable
10	Patch Management solution	Not Applicable	Not Applicable

The bidder should recommend appropriate bandwidth to meet the stipulated RPO and RTO.

i. **Implementation of DR Policy**
The Bidder should prepare and submit a detailed implementation plan with mapping of infrastructure at DC site and DR site. The bidder is also required to provide all necessary SIT-NET related assistance for conducting DR drills as per SEBI's IT & BCP policies.

ii. **Testing**

After implementing the DR-BCP solution, solution partner should test all the process / application individually, in group and in totality. Following should be included in the testing of the BCP, but not limited to:

i. Crisis command team call-out testing
ii. Technical swing test from primary to secondary work locations
iii. Technical swing test from secondary to primary work locations
iv. Application test and migration test plan of each application data/logs generated
v. Business process test

iii. BCP testing Schedule:

Solution design should include BCP/DR test / drill once in 6 months after successful implementation of BCP/DR to be carried out by solution partner. Problems identified in initial testing phase or any test/drill should be rolled in planned and time bound manner.

iv. Documentation:

Documentation of the Disaster recovery plans should include, but not limited to following:

i. Data replication methodology between primary and secondary work sites
ii. Applications/ call migration methodology between primary and secondary work sites
iii. The application and software required at the secondary work site, and
iv. The type of physical data requirements at the secondary work site.

b) **Local Survivability:** The proposed solution architecture must support Remote Survivability feature (Local Survivability) where, if Remote location (Other than SEBI HO i.e. SEBI Regional offices or SEBI Local offices) gets disconnected (by means of MPLS/Internet connectivity failure/device failure) from DC and/or DR, the solution should continue to work with limited features that are locally supported by the gateway or server. **The bidder should identify and provide the list of applications available as local survivability. Proposed list of application wise local survivability work solution component proposed as part of SIT-NET project is mentioned below:**

Table 3: Local Survivability Components

Sr. No.	Device/Technology
1	All LAN items in the SIT-NET bill of material, that are at any RO or LO of SEBI (Network Devices etc.)
2	Firewall
3	Wi-Fi
4	IP Telephony (LAN)
5	AD, DNS , DHCP
6	Video Conferencing

2.2.6. Network and Security:

a. The bidder will be responsible for supply, installation and Commissioning of SIT-NET to ensure enterprise-wide accessibility as per defined SLA's. The bidder shall be responsible for ensuring security of SIT-NET from any threats and vulnerabilities. The bidder shall address ongoing needs of security management including, but not limited to:

1. monitoring of various devices/tools such as firewall, intrusion prevention/ detection
2. content filtering and blocking
3. virus protection
4. event logging & correlation
5. vulnerability protection through implementation of proper patches and rules.

<u>**The bidder should also ensure compliance to various Government/MeitY directives/ Cert-in advisories/ requirements for certain infrastructure/devices.**</u>

b. Zero Trust Model:

i. Bidders are required to propose a suitable solution which would help SEBI maintain Zero Trust Model within SIT-NET. The solution should clearly articulate the network architecture stating movement of encrypted data and traffic both East-West and North-South direction.

ii. Bidders are to configure Zero Trust network architecture at SEBI and all the required ports, softwares, customization required to achieve the same needs to be provided by bidder.

c. The solution should leverage the current SOC-NOC of SEBI and be guided with current security framework and tools (specifically SIEM, PIM, EDR-EPP, NMS). Bidder is required to integrate all required infrastructure with NOC & SOC as applicable. Bidder may propose a detailed strategy for same. Detailed list of technologies to be integrated with NOC SOC is enclosed at appendix XII.

2.2.7. Performance Monitoring and MIS Reports:

The Bidder shall integrate SEBI's Network Monitoring Solution (Everest) (Refer Appendix XII Point no 23 and 24) covering all the proposed technologies for measuring the service levels, performance and utilization of Network applications, Network devices (Servers, Routers, Switches, Firewalls etc.) and other network components and provide single view and management reports. The bidder should configure and if required customize such that the tool should be capable of followings:

i. Generating periodic reports (weekly, monthly, quarterly reports) having Baseline performance, Low performance, Adverse performance and Breach along with the SLA credit points as mentioned in clause Appendix X-point 13-Annexure B-SLA calculation).

ii. Generating various reports like Executive report, detection life cycle report, End Point Compliance Report, Top 10 reports for various category and Health reports etc.

iii. Reports with (but not limited to) HTML/CSV/PDF/Excel formats.

2.2.8. Standards: Compatibility and Interoperability

Compliance process should be as per the defined international standards and security guidelines such as ISO 27001:2013, ISO 27032, ISO 17799, ISO 22301, COBIT5, MAS etc./NIST Framework/Guidelines issued by SEBI to MIIs, for maintaining operations of SIT-NET from time to time. The solution deployment should be compliant with SEBI's IS, IT and Cyber policies, internal guidelines, regulatory requirements and country wide regulations and laws from time to time. Deployment Process and Compliance of the same to be followed as per Process and Security guidelines provided in most recognized and followed International Standards and Guidelines issued by SEBI. The proposed and implemented solutions should be compatible and interoperable with each other within SIT-NET.

2.2.9. Maintenance and Support:

The Bidders are expected to build a self-reliant architecture that requires minimal monitoring and support. Bidders should adopt suitable automation tools for maintenance and support so as to optimize the number of resources deployed on site. The Bidder should provide adequate support for SIT-NET Management both at Primary Data Centre and DR site to meet the stipulated SLA. It is expected that bidder will factor in back to back support with OEM to ensure speedy turnaround time in case of any of the proposed system failure. For details refer to clause 2.4.

2.2.10. Versions, Upgrades and Updates:

All patches, upgrades, updates of software components should be provided during the entire tenure of the agreement. The price of the same should be included in the proposed Bill of Material (BOM). The Bidder should quote all the latest versions (current line) of products, software, hardware's, servers, appliances, etc. **The quoted products, software, hardware, servers, appliances, etc. should not be declared as end of support during the period of agreement from the date of agreement**. **SEBI also proposes to upgrade to one stable higher version on the 3rd year of warranty prior to initiation of AMC.**

2.2.11. Licenses:

The licenses for all the proposed products/solutions should be in the name of SEBI and should be valid during the tenure of the agreement. SEBI may further extend the quantity to additional user licenses for all the proposed products/ solutions on quoted rates as and when required during tenure of the agreement. The bidder should be able to use existing perpetual licenses available with SEBI, if any.

2.2.12. Site Survey:

Prior to bidding, the bidder should conduct site survey of the data centre, all SEBI offices including ROs, LOs and suggest SEBI the infrastructure requirements including but not limited to power requirement, cooling requirement, internet bandwidth requirement etc. and should submit a certificate confirming the same (refer Form 13). The bidder should execute a Confidentiality and Non-Disclosure Agreement as also an Undertaking inter alia that they shall not disclose any information acquired while dealing with the Project which is confidential in nature to anybody including their relatives.

The bidder should use latest cabling like Cat 6A and Cat 7 wherever required to connect.

2.2.13. Risk Assessment, Mitigation and Audit:

i. Bidder has to undertake a complete Risk Assessment of current state including vulnerability assessment and Penetration Testing (VAPT) by every six months or as per SEBI's discretion for the SIT-NET solution and submit the reports on VAPT and undertake corrective actions.

ii. The VAPT should be conducted by Cert-in empanelled agencies and the agency should submit its Cert-in empanelment validity certificate to SEBI.

iii. Create and modify the existing Information Security Policy for SEBI SIT-NET solution.

iv. Provision to provide the audit logs to SEBI NOC-SOC to identify any unauthorized access to SEBI's systems. Capability to support storing log files for duration of project in a durable and inexpensive storage solution.

v. **Governance and Compliance:** Capability to discover all of SIT-NET resources and view the configuration of each. Receive notifications each time a configuration changes, Capability to obtain details of what a resource’s configuration looked like at any point in the past.

2.2.14. Migration Plan:

The bidder is expected to carry out migration of existing IT Network infrastructure both at DC and DR (as per the BOM [Appendix III]). The migration activity may include porting of existing functionalities, configuration, call logs, user data, statutory access logs, AD, DNS, DHCP data, IP Telephony user details, User IP Phone configuration, AD users, VPN users etc. to the new system where applicable. The bidder is required to submit a detailed Migration plan including resources and efforts to undertake migration activity. It is expected that the migration should be non-disruptive across all offices of SEBI. The bidder should be responsible for migration of existing old system to the new system with zero downtime.

2.3. Functional and Technical Specifications

The Functional Specifications of the SIT-NET includes but not limited to the following features:

i. Centralised management of Network Components, IP Telephony, Switches, Routers, Wi-Fi, Firewalls and Video Conferencing solution etc.
ii. 40 Gbps Back Plane for internal core network infrastructure and 10 Gbps for all other network infrastructure.
iii. Software Defined Network Infrastructure across SEBI offices
iv. Network Access Control across SEBI offices
v. Centralised AD, DNS, DHCP services deployment across SEBI offices
vi. Centralised implementation and management of Wireless access
vii. Auto Shift to DR in case of failures.
viii. Connectivity to NOC/SOC solution as required with a capability to automatically orchestrate advises from NOC SOC system.
ix. System must support NTP time synchronization (client mode) to multiple servers.
x. Solution must support GUI & CLI based configuration.
xi. There should be no single point of failure in the proposed solution; the failure of one or more components of the solution should not affect the organizational network's functionality i.e. Solution should work in offline Mode /SPAN/ Mirror Traffic.
xii. The solution should be IPv4 & IPv6 compatible.
xiii. All suitable measures to be in place to ensure Zero Trust Model ('No unauthorized Access') while the traffic is moving over MPLS / WAN etc.
xiv. Local Survivability

Note 4: Bidders are expected to be guided by solution wise principles listed in RFP. Bidders may choose to provide additional functionality in accordance to their proposed solution and product line.

Detailed functional and technical specifications are present at Appendix VI. Solution Specific specifications are as follows -

2.3.1. Solution for Network Devices

The solution for Network Devices comprises of connectivity devices like router, switches, Load Balancer etc. The proposed solution should cover Network Connectivity Devices having features including but not limited to the following functional principles:

i. The Network devices should support graphical user interface (GUI) with dashboards for Management.
ii. The Network devices should be compatible with Simple Network Management Protocol Version 3 (SNMP v3).
iii. The Network devices should be having Stacking capabilities.
iv. The Network devices must be having POE (Power on Ethernet) capability.
v. The Network devices should generate and provide Real Time Multi-Port Statistics on the graphical user interface (GUI) dashboards.

vi. The Network devices should have Zero Touch provisioning (Plug and Play) when connected in SIT-NET.

vii. All suitable measures to be in place to ensure 'No unauthorized access' while the traffic is moving over MPLS / WAN etc.

viii. **Link Load Balancer:** The Link Load Balancer solution is required to be deployed in High Availability architecture in Head Office, in order to have complete redundancy as per SEBI's Network & Security design requirements.

ix. **Network Racks:** All the Racks have to be supplied for Data Centre deployment only. For floor hub rooms, SEBI's existing racks would be utilized. SEBI expects that the proposed solution architecture should be optimized in terms of cooling, power, and space (number of racks) requirements. In terms of space it is expected that solution will be implemented in no more than 5 racks.

2.3.2. Solution for IP telephony

The proposed IP Telephony solution should be a converged communication system with ability to run TDM and IP on the same platform using same software load based on the server and Gateway architecture. The proposed IP Telephony solution should be having features including but not limited to the following functional principles:

i. The solution should provide the below mentioned IP phones along with relevant licenses for hardware as well as soft client (licenses) facility on all the IP Phones:

Table 4: Types of IP Phones

Sr. No.	Type of IP Phones
1	Video IP Phone for Division Chiefs
2	Video IP Phone for Senior Management
3	Non-Video IP Phone for Officers
4	Non-Video IP Phone for Outsource Staff (Data Entry Operators, Electrician, Pantry, SEBI Control etc.)
5	Non-Video Conferencing IP Phone for Conference Rooms

ii. The IP Telephony solution should be capable of supporting open standard protocols and support traditional telephony interface such as Analog and IP/Digital, PRI extensions, Trunk interface etc.

iii. The solution must be deployed in a virtualized platform.

iv. The solution must provide soft-client facility for Video, Audio calling, Instant Messaging and Presence within SEBI network and outside SEBI network as well from Day 1.

v. The solution must connect IP Telephones connectivity across all SEBI offices (HO locations, ROs, Los).

vi. The solution must integrate with a dedicated Voice gateway for PRI/PSTN calling over MGCP or SIP protocol at each location.

vii. The solution should have local survivability. The solution must support local Gateway based redundancy for IP Phones and soft phones in case of non-reachability to the central infrastructure.
viii. Entire solution must support IPv4 & IPv6 from Day 1.

2.3.3. Solution for Wi-Fi accessibility

Wi-Fi Solution should provide centrally managed Wi-Fi solution at SEBI premises. The solution will have to be extended to all SEBI office locations. Bidder has to roll out centralized managed Wi-Fi Solution in all premises of SEBI (including ROs and LOs).

The Proposed solution should provide multiple levels of access for users, managers, administrators etc., depending on rules and roles. Solution should be scalable and MFA authentication must be provided. The solution should have a capability to provide all user WIFI connectivity without any disturbance. The solution should be user friendly. The bidder will install Wi-Fi solution hardware, software at required locations and will make the system available to all SEBI office locations. The proposed Wi-Fi solution should be having features including but not limited to the following functional principles:

i. Centralized Authentication through AD.
ii. Wireless access has to be provided based on user role, user groups, based on multiple parameters of AD so that any kind of customized group policy can be pushed
iii. Rule based controls should be from SEBI's systems and not bidder's cloud based (unless SEBI's IS policy provides for this)
iv. Configurable capability for defining SSID to specific Access Points
v. Automatically shift to adjacent access points if the load is high on particular access points
vi. Packets are encrypted end to end.
vii. Wireless intrusion detection/prevention systems should identify and block following but not limited to
    a. Ad-Hoc Network
    b. Dis-association of AP/Client to other network access points.
    c. Rogue access points detection & prevention
    d. Multiple failure attempts to connect to the wireless network/man in the middle attack.
    e. Honey Pot attacks.
    f. DOS attacks etc.
viii. Bandwidth restriction per user/on group
ix. QoS throughput traffic prioritization
x. Solution shall have MFA based Authentication

2.3.4. Solution for Software Defined Network

The intent to implement Software Defined Network is to incorporate centralized management and visibility of SIT-NET’s solution. The proposed SDN solution should have features including but not limited to the following functional principles:

i. Software defined solution for centralized configuration, management and monitoring. The solution should support software defined automation and network device life-cycle management. Solution should be capable of plug and play configuration and template based network provisioning. Solution should support advanced wireless troubleshooting using wireless sensors.

ii. The solution should have Zero Touch provisioning (Plug and Play) when connected in SIT-NET. Solution should have Automated network devices on-boarding. The system should allow for plug and play installation of network devices without requiring any manual configuration.

iii. Identifying and monitoring Network Topology within site location.

iv. Encryption of network traffic getting generated within SIT-NET. MACsec based Encryption of network traffic between switch to switch and IP sec based encryption between Firewall to Firewall within SIT-NET.

v. The solution should provide functionality to select preferred version of software image and highlight devices deviating from preferred version. System should support GUI based upgrade of switches deployed in SIT-NET.

vi. Troubleshooting the network slowness/access issues using analysis of network traffic.

2.3.5. Solution for Network Access Control (NAC)

The intent to implement Network Access Control Solution to enforce policies on devices that access SIT-NET, to have complete network visibility and mitigate risk. The proposed NAC Solution should cover including but not limited to the following functional principles:

i. Onsite Installation and implementation of the solution at DC and DR.

ii. Dedicated policy management to define and administer security configuration requirements, and specify the access control actions for compliant and noncompliant endpoints. In order to have better control and visibility of unauthorized systems connecting to SEBI network, all the network switch ports, especially those which are connecting to endpoints (user PCs) should be blocked and alerted while any unauthorized devices trying to connect to SEBI network.

iii. Ability to conduct a security state baseline for any endpoint attempting to connect and determine the suitable level of access.

iv. Access control so we can block, quarantine or grant varying degrees of access.

v. The Solution should **detect and block** the unpatched, unauthorized systems or devices without proper security softwares (such as antivirus, etc.) when connected to SEBI’s network. Example of unauthorized systems are: visitors/outsiders/employee owned personal computers/laptops/mobile phones/iPads/other networking/ Wi-Fi/ Bluetooth devices/ other handheld devices, etc. and servers/devices/networking equipment's of other third party organizations / contractors /service providers /individual trying to connect to SEBI's network.

vi. The solution should automate the process of on-boarding networking devices automatically with minimum manual interventions.

vii. Integration with other NOC-SOC applications and components like SIEM, Anti-APT, Antivirus, AD etc.

viii. Solution shall use agent-based and/or agentless approach for detection of unauthorized access to the network.
ix. Solution shall provide forensic evidence on any unauthorized access activity within the network.
x. The proposed solution should support local survivability.
xi. NAC should support all SEBI inventory.

2.3.6. Solution for AD, DNS, DHCP

SEBI intends to implement a unified and scalable AD, DNS, DHCP & IP Address Solution (DDI) solution. It is intended to have all three components (DNS, DHCP & IP Address Management) to be deployed and centrally managed. Proposed DDI Solution preferably should run all modules together on single appliance. DDI Solution needs to be deployed at DC & DR. DR site should be capable of handling 100% load during the failure of DC. The proposed Solution should cover including but not limited to the following functional principles:

i. Updating of AD files – to be updated and synced with SEBI's SAP feed file on a daily basis.

ii. Setting up of Active Directory /DNS server at HO and DR in high availability mode and single instance at ERO, WRO and NRO.

iii. Setting up of DHCP and Certificate server at HO (SEBI Bhavan 1 and SEBI Bhavan 2) and DR in High availability mode, and single instances at Regional offices (Delhi, Kolkata, Ahmadabad and Mittal court)

iv. The implementation of AD/DNS/DHCP services should be compatible and interoperable within SIT-NET.

v. The solution should have local survivability.

vi. Self Service portal for user's password reset and other functionalities to users using MFA and secret question.

vii. System must support monitoring using SNMP v3

viii. System must integrate with multiple pass-through authentication options including RADIUS, LDAP, Active Directory, SEBI's SAP HR system (Feed file) etc.

ix. The implementation should also include setting up Group policies, integration and all the necessary components, etc.

x. Proposed solution should be vendor agnostic for integration with network devices (Switch/Router etc.) (solution should not have any dependency on any Network switches/router OEM to operate smoothly).

2.3.7. Solution for Network Security [Firewalls]

Note 5: This solution should integrate with SEBI's existing NOC-SOC solution. Setting up additional SOC/NOC is not intended as per the requirement of the RFP.

The proposed Network security solution comprising of Next-Generation firewalls and other related security components should cover including but not limited to the following (functional principles highlights only capabilities proposed):

i. Security Devices (Firewalls and related equipment) of Next Generation firewall features and appropriate configuration should be implemented across all SEBI offices including ROs and LOs.
ii. Management of Network security infrastructure and services using web based interface, threat detection and incident response and implementation of the solution at DC and DR.
iii. Threat Prevention using sandboxing, anti-phishing, anti-virus, anti-bot, analytics and threat intelligence. Focus on blocking malware and application-layer attacks, along with an integrated Intrusion Prevention System (IPS).
iv. Solution should have built in capabilities to react quickly and seamlessly to detect and react to outside attacks across the SIT-NET and add exceptions for detections.
v. Set policies to defend SIT-NET and carry out quick assessments to detect invasive or suspicious activity, like malware, and shut it down.
vi. Protect in-scope systems from the Internet and from other parts of the SIT-NET's environment. Configure these systems with security policies that deny all traffic except that is required for production applications, and can also apply threat prevention controls required to be in compliance.
vii. Application based Inspection and control, Identity based Inspection and control.
viii. Solution shall provide forensic evidence on any unauthorized access activity within the network as follow: Event timestamp, network events in sequence, packet capture of suspicious communication, malware behaviours, malware type, severity, source and destination of attack.
ix. The proposed solution should support to monitor traffic from multiple segments like WAN, DMZ, Server Farm, Wi-Fi network, MPLS links etc. simultaneously on a single appliance.
x. Location wise Firewall solution distribution is mentioned in below table:

Table 5: Location wise Firewall Distribution

Sr. No.	Location	City	Firewall (Traffic) Type	Firewall Capacity	Deployment mode
1	SEBI Bhavan 1	Mumbai	Internal	10 Gbps	High availability
2	SEBI Bhavan 1	Mumbai	External	10 Gbps	High availability
3	SEBI Bhavan 2	Mumbai	Internal	10 Gbps	High availability
4	SEBI Bhavan 2	Mumbai	External	10 Gbps	High availability
5	DR-Chennai	Chennai	Internal	10 Gbps	High availability
6	DR-Chennai	Chennai	External	10 Gbps	High availability
7	Mittal Court Office	Mumbai	Composite (Internal and External-Both)	3 Gbps	Single device
8	NCL office	Mumbai	Composite (Internal and External-Both)	1.5 Gbps	Single device
9	ERO	Kolkata	Composite (Internal and External-Both)	3 Gbps	Single device
10	WRO	Ahmedabad	Composite (Internal and External-Both)	3 Gbps	Single device
11	NRO	New Delhi	Composite (Internal and External-Both)	3 Gbps	Single device
12	Local offices	Across SEBI	Composite (Internal and External-Both)	1.5 Gbps	Single device

2.3.8. Solution for Virtual Private Network (VPN)

The solution should implement SSL VPN for Secured Remote Access for providing secure, reliable transport over internet; this will include device rules / device policy definition and enforcement on the appliances. It is envisaged that VPN solution should have atleast following 3 use cases-

i. Access to development environment for developers.
ii. Adhoc data collection or upload through API or SFTP, etc.
iii. Work from Home.

The proposed VPN solution should cover including but not limited to the below functional principles:

i. Onsite Installation and implementation of the solution at DC and DR.

ii. Provide SEBI users (Permanent and Outsourced[4]) with secure remote access (RA) to take advantage of VPN infrastructure service.

iii. Should have provision for various features facilitating Work from Home facility.

iv. The solution must support a wide variety of endpoint devices and operating systems (Example: Windows, MacOS, Linux etc.).

v. The solution must provide seamless access to the internal network and public data resources from managed and BYOD devices.

vi. The solution must ensure to Authenticate and Policy control that integrates with the authentication resources in use by the organization.

vii. The solution must provide Cryptographic security to prevent the exposure of sensitive data to unauthorized parties who accidentally or intentionally intercept the data.

viii. The solution must provide the mentioned features such as User authentication, self-service facility like password reset, differentiated access, Strong encryption for data privacy, hashing for data integrity, Split-tunnelling, Device resiliency, Internet link resiliency, Web Deployment, Advanced Malware and DNS protection, VPN Load Balancing etc.

ix. Solution should be scalable (Refer to section 2.2.2 Capacity and Sizing).

x. Self-service portal and Multi factor authentication. OTP should always be generated as 3rd factor authentication.

xi. Provide split tunnelling features.

2.3.9. Solution for Video Conferencing

The proposed Video Conferencing solution should cover including but not limited to the following fundamental principles:

---

[4] Outsourced users including technical support staffs, Interns etc.

i. The solution should be able to deploy hybrid Video architecture using IP based ‘On-premise infrastructure’ (Video End-Points) and ‘Cloud based’ platform like WebEx, MS Teams etc.

ii. The High Definition Video Conferencing (HDVC) Infrastructure to schedule, conduct and manage Video Conferences centrally, (Mobile and Desktop based) over SEBI Network in a secure way. Solution should allow any HDVC end point to Join any cloud-based providers like WebEx, MS Team, Zoom, Google Meet over SIP/H.323 standard based protocol etc.

iii. The video conferencing facility should be extended to Webinar and Webcast.

iv. The HDVC end point should be able to provide plug and play facility so that a Computer (Laptop/Desktop/Other similar devices like Digital Tablets) can be connected to the web based video conferencing applications and use the camera and audio-video features similar to the HDVC end points. The solution must provide Video conferencing end-points devices/units for different capacity rooms like Mid-sized conference rooms (6-10 seaters) and Large Conference rooms (More than 10 seaters).

v. For Large Rooms, the dedicated codec based video conferencing end points have to be provided.

vi. For Mid-sized conference rooms, Plug and Play (USB type high definition video camera and Audio units) video conferencing devices have to be provided.

vii. Movable VC units along with the required cable extension and trolley.

viii. The solution with two (2 different OEMs) cloud based/software-based video conferencing facilities must be deployed with organization wide licenses for meeting/webinar/event/webcast.

Sr. No.	**Type of VC Solution Categories**
	Hardware based VC solution
1	Codec based Video End-Points for Large Rooms
2	Plug and Play (USB type high definition video camera and Audio units) based Video devices for Mid-sized rooms
3	Movable VC units along with the required cable extension and accessories
	Software based VC solution
4	Software based video conferencing solution (OEM 1) for Video conferencing meetings (Department/Division based) having minimum 1000 participants in a web conference.

5	Software based video conferencing solution (OEM 1) for Video conferencing meetings (Individual basis) having minimum 100 participants in a web conference
6	Software based video conferencing solution (OEM 2) for Webinar and webcasting having minimum 3000 participants in a web conference

ix. The solution should preferably integrate with the IP Telephony platform with centralized phonebook, centralized dial plan, and point to point & multi point calling between IP Phones, HDVC endpoints & soft clients.

x. Dedicated On Site FMS support should be provided at Head office and on-call basis to Regional offices and Local offices when required.

xi. Entire solution must support IPv4 & IPv6 from Day 1.

2.3.10. Solution for Patch Management

The bidders are required to propose a suitable Patch Management Policy and accordingly provide an appropriate Patch Management solution for SIT-NET. The bidders would undertake the Patch Management for all network devices based on the proposed Patch Management Policy. The Patch Management solution would be scalable and flexible to cover SEBI's endpoint devices as well, though, the bidder's responsibility will be restricted to provide timely patches to the infra provided by them.

The bidder should set up and implement the Patch management solution for patching LAN/WAN desktops and servers. The solution should be set up at Primary data center and all the endpoints (PC's/Servers etc.) connected to the LAN/WAN/Head Office/Regional Offices/Local offices should get the updates/patches from this centralized solution. The Patch management solution should be able to patch Windows/Linux and other types of operating systems. The solution should also facilitate remote installation/remote pushing of softwares across connected desktops/servers of LAN/WAN network. The solution shall have the following features.

i. Integration with SEBI's Active Directory
ii. Integration with various systems and solutions implemented across SEBI to fetch the inventory of the endpoints within SIT-NET
iii. Asset and Inventory Management
iv. License Metering
v. Software Distribution
vi. Configuration Management

2.3.11. Solution for Work from Home

The proposed solution should be integrated with VPN solution (Refer 2.3.8). Bidder is required to propose a scalable WFH solution having but not limited to the following features:

i. Work From Home solution should be designed for the employees of SEBI who are desirous to remotely access office infrastructure.
ii. Remote management and support for users

Bidder may refer specification of VPN solution to provide above functionality.

2.3.12. Solution for BYOD

Bidder is required to provide a suitable BYOD solution using the required technology. The Solution should be scalable and include secured BYOD access for various kind of devices (laptop, mobile, Tablets, etc.) including various Operating system (Windows, Android, iOS, Linux, etc.). Present BYOD policy is enclosed at Appendix XVI.

Bidder may refer specification of Wi-Fi solution, NAC, VPN solution and other relevant solutions to provide above functionality.

2.4. Deployment of Resources

2.4.1. Deployment of Resources during implementation

i. It is expected that bidder will deploy adequate trained and experienced manpower during the implementation of the project. Bidder will be required to deploy requisite number of personnel to implement the SIT-NET solution. Though SEBI has stipulated minimum number of resources, bidder is required to deploy adequate (Over and above the minimum stated) resources to meet the implementation timelines and post implementation SLAs as per their own estimates.

ii. The Proposal is expected to meet the minimum resources during the implementation stage (For details refer to Appendix IV: Manpower Requirement). Bidders would be required to submit in details the job responsibilities to be undertaken by these resources. Bidder should define the exact number of resources along with their key responsibilities and types of resources needed on-site.

iii. Bidder should provide qualified and experienced resources to work on-site during the implementation period.

iv. Bidder has to arrange alternate resource of similar qualification and experience in case when the deputed resource is unable to report to SEBI due to various reasons to meet the implementation timelines of SIT-NET solution.

v. SEBI may conduct interview for the manpower deployed during FMS support pre & post implementation. Before implementation, SEBI may conduct interview of Project Manager, Solution Architect, Technology Manager. Bidder to submit resume and other details of the mentioned personnel.

2.4.2. Post-implementation

i. Post GO-Live, Bidder shall deploy requisite number of personnel to maintain the SIT-NET system. Total cost of these resources shall be part of the Bill of Material (BOM).

ii. Bidder shall deploy additional resources as and when required.

iii. Bidder has to arrange alternate resource of similar qualification and experience in case when the deputed resource is unable to report to SEBI due to various reasons to sustain the day to day activities and provide efficient support for SIT-NET.

iv. Bidder should provide qualified and experienced resources to work on-site during the contract period: (Refer to Appendix IV **Manpower Requirement**)
   a) Minimum 5 L1 engineers at HO (SEBI Bhavan 1 and SEBI Bhavan 2).
   b) Minimum 1 L1 engineer at each RO.
   c) Minimum 2 L2 onsite engineer at HO.
   d) Minimum 1 L3 engineer-on call basis.
   e) Support for other SEBI offices including LOs on call basis.
   f) Minimum 3 Helpdesk staffs at HO.
   g) Minimum 4 L1 engineers for video Conferencing at HO and on call basis at ROs and LOs.
   h) Minimum 1 Technician for maintenance and repairing of hub room, data centre, cabling, troubleshooting etc.

v. **Shift Timings:**

Sr. No.	**Location**	**Shift Timings**	**Days**
1	SEBI HO (SEBI Bhavan 1 and SEBI Bhavan 2, Mittal Court, NCL office)	2 (two) shifts operations (8 AM to 8 PM)	Monday to Friday
2		1 (one) shift operations (09: 30 AM to 05:30 PM) **To be used for Preventive Maintenance**	On Saturday
3	SEBI Regional Offices	1 (one) shift operation (09:30 AM to 05:30 PM)	Monday to Friday

The shift timings mentioned are indicative however these may vary w.r.t. work and load or as per SEBI's discretion.

It may be noted that the support person may be deputed at other office locations of SEBI (Within Mumbai) if required.

vi. Bidder would play a critical role in on-going support. Replacement of a resource under unavoidable circumstances needs to be intimated to SEBI in advance and the replaced resource should be equally or more qualified and experienced.

vii. The details of work, responsibility and competency of the resources are available in Appendix IV.

viii. Preventive Maintenance: SEBI envisages following preventive maintenance activities after go-live.

Table 6: List of maintenance activities

Sr.No.	Activity Detail	Frequency of Delivery
1.	System Hardening	As and when required
2.	Update/Upgrade/Patching	As and when required
3.	Backup/Restore	As per the policy defined by SEBI
4.	Configuration Management	As and when required
5.	Configuration Review and Performance Tuning	Quarterly or As and when required
6.	Change Management	As and when required
7.	Access Management	Continuous
8.	SIT-NET Manual /SOP Preparation and Review	During Implementation of SIT-NET Solution (Baseline Manual), Half Yearly
9.	Security Device Problem	As and when required
10.	DR Drill of SIT-NET	As and when requested by SEBI
11.	Security Inventory Management	Continuous
12.	License & AMC Management	Continuous
13.	OEM/SI Liasoning for technical support	As and when required
14.	Custom policies	As and when required
15.	Integration with IT / IS infrastructure (Existing/Future)	As and when required
16.	Monitoring policies	Continuous
17.	Custom Reports	As and when required
18.	OEM/SI Coordination for Support	As and when required
19.	Data Centre and Hub room physical status check	As and when required (At least weekly once)

20.	Verification status of Integration of network devices/solutions with SEBI's SOC-NOC and other technologies/solutions	As and when required (At least quarterly once)

2.5. Sizing Specification of SIT-NET

i. Sizing specifications are based on certain calculations and assumptions (refer clause 2.2.2. Capacity and Sizing). These are based on minimum sizing specifications/requirements to be met in response to the RFP. The Bidder should not rely entirely on the below mentioned information to design and propose their products/ solutions to SEBI. They should make their own calculations, investigations, decisions to size their products/ solutions/services appropriately to meet the requirements of the RFP (such as Redundancy, high throughput etc.).

ii. The bidders are requested to ensure proper sizing of the solution based on their overall assessments, scope of work defined in RFP and other parameters such as SLA requirements, etc.

iii. The Bidders should consider existing IT set up (refer Appendix III-Present IT Set up) for considering solution design, architecture, licenses, device licenses, storage, backup, archival, connectivity, number of ports /segment requirements in appliances/devices, etc. while proposing SIT-NET as per the requirements of this RFP.

iv. For Sizing requirement for DC and DR (refer clause 2.2.2. Capacity and Sizing).

2.6. Responsibility Matrix

The Responsibility Matrix showing the responsibility of Bidder and SEBI is attached at Appendix VII **Responsibility Matrix.**

2.7. Log Retention

i. All Log (raw or Normalized) data must remain within SEBI's Data Centre. Under no circumstances these data must travel outside SEBI's environment. Further, Bidder must follow the best practices for all compliances related to data and it's security. Bidder will be responsible to store logs in industry standard solution and format.

ii. Bidder shall propose solution that should be capable of retrieving the archived logs for analysis, correlation and reporting and forensic purposes.

iii. Log retention period must be Six Months – Online.

iv. After the online log retention period, logs must be pushed to centralized solutions as decided by SEBI for archival purpose.

v. Bidder must ensure that once the logs are written to the disk/ database, no one including database / system administrator should be able to modify or delete the stored raw logs.

2.8. Training

The bidder will be responsible for training SEBI's IT team as and when required in the areas of implementation, operations, management, monitoring, error handling, system administration etc. The training will be given both during-implementation and post-implementation for proposed solution.

The cost of lodging and boarding, when training is conducted outside Mumbai, will be borne by SEBI.

i. The Bidder shall give adequate training to the officials of SEBI during implementation of the project. The Bidder shall provide the training exclusively for selected products being delivered and should necessarily cover the products supplied to meet the functional and technical specifications mentioned in the section 2.2 above. The training schedule, for providing necessary and adequate training to SEBI's personnel, must be finalized in consultation with SEBI, and will form a part of the agreement/ contract. The details of the training to be provided in each category shall be clearly stated in the offer. Each participant should be provided with the copies of training material. Boarding and lodging cost for SEBI officers attending the training will be borne by SEBI.

ii. **During Implementation:** Training will be provided to SEBI IT team on the product architecture, functionality and the design for each solution under the scope of this RFP.

iii. **Post Implementation:** Training will be provided to SEBI IT team on operations, alert monitoring, security orchestration, policy configuration for all in-scope solutions, routine operations, management, monitoring, etc.

iv. The Bidder shall train SEBI 's IT Team for independent operation, creation of policies/rules, generation of reports, and analysis of the reports, troubleshooting and familiarization of features and functionalities, policy configuration, alert monitoring.

v. The bidder and OEM are required to provide ad-hoc trainings to SEBI staff, to acquaint them with the latest features and functionalities of the solutions for minimum of one day. SEBI has the right to exercise this training option at its discretion.

vi. The OEM Certified training where applicable for the identified technologies (Refer to 3.2.1. E), should be provided by respective OEMs for at least 5 SEBI IT persons every three year till the tenure of the agreement i.e. two times during the tenure and should also facilitate to undergo formal certification program conducted by respective OEMs without adding any additional cost to SEBI.

vii. The Solution partner's response should clearly indicate the following details related to OEM certified training (as per Appendix I Form 17) in the technical bid:

a. OEM name
b. Product /solution/service name
c. Topic of the training
d. Number of days
e. Tentative location
f. Nature of training
g. Training material
h. Certification, if any

viii. **SEBI proposes to hold one-day orientation program on the implemented technologies for senior management at the location specified by SEBI.**

2.9. Technical proposal

The Bidder would be required to submit a technical proposal including the following listed items but not limited to:

i. Past relevant experience including technical capabilities to implement this project

ii. Key features of the proposal (Refer clause 2.2.i)

iii. Integration approach with other IT Infrastructure like Share Portal, SEBI private cloud Infrastructure, IMSS/DWBIS infrastructure, etc.

iv. Proposed training and capacity building at SEBI

3. Bid Evaluation Process

3.1. Evaluation Process

a. SEBI will constitute a committee to evaluate the responses of the Bidders (Bid/Tender Evaluation Committee).

b. The Bid Evaluation Committee constituted by SEBI shall evaluate the responses to the RFP and all supporting documents/ documentary evidence. Inability of a Bidder to submit requisite supporting documents/ documentary evidence within a reasonable time provided to it, may lead to the Bidder’s Proposal being declared non-responsive.

c. The decision of the Bid Evaluation Committee in the evaluation of responses to the RFP shall be final. No correspondence will be entertained outside the process of negotiation/ discussion with the Bid Evaluation Committee.

d. The Bid Evaluation Committee reserves the right to reject any or all Proposals on the basis of any deviations contained in them.

e. Each of the responses shall be evaluated as per the criteria and requirements specified in this RFP.

f. The bids will be evaluated first on the technical merits and then on commercial merits and SEBI’s decision in this regard shall be binding, final and conclusive.

g. Each bidder will have to present the proposed solution’s architecture diagram, and details of software stack, hardware stack (compute, Storage, Network), Backup etc. to the Technical committee of SEBI for evaluation.

h. SEBI will bear all the cost of travelling, lodging, boarding etc. of its Bid Evaluation Committee and its officials in relation to reference customer site visits and POC evaluation.

i. Bidder must provide masked BOM as exact replica of price bid. Bidder has to submit undertaking to this effect.

3.2. Technical Evaluation

The bid document will be evaluated as per the requirements specified in the RFP. The Bidder is required to submit all required documentation in support of the functional specification criteria specified. Technical presentation will be a part of the process.

Each Technical Bid will be assigned a technical score out of a maximum of <400 Marks> marks. Only the bidders with overall score of more than 75% and score of more than 65% in each of the Evaluation Criteria mentioned in section 3.2.1 components will be technically qualified and short listed for commercial evaluation. Failing to secure minimum marks shall lead to technical disqualification of the Bid.

3.2.1. Scoring Model

The Bidder's technical proposal will be evaluated as per the requirements specified in the RFP and adopting the following evaluation criteria-

Table 7: Evaluation criteria

Section	Evaluation Criteria	Total Marks
A	Bidders Compliance to Functional and Technical Requirement Specifications	120
B	Bidder Capability including Proven Relevant Experience	80
C	Understanding of SEBI's requirement and Presentation to TEC (Tender Evaluation Committee)	100
D	Proof of Concept	80
E	Training	20
	Total	**400**
	Over all Qualifying Marks	75%
	Qualifying marks for each section	65%

The detailed scoring model is given below –

A. Bidders Compliance to Functional and Technical Requirement Specifications (120 marks)

i. Bidders are required to strictly adhere to the principle functionalities mentioned in clause 2.3 w.r.t. each of the technologies mentioned in the following table no.8.

ii. Bidders are required to propose solution for **ALL** the technologies mentioned in the following table no. 8 failing which their solution will not be assessed.

iii. Scoring will be done based on submission as per Appendix VI. For each specification 1 mark is allotted. For each mandatory specification 2 marks are allotted. Total marks obtained for each technologies will be appropriated w.r.t. the maximum marks mentioned in the following table no. 8.

Table 8: List of Technologies and Solutions

Sr. No.	List of Technologies and Solutions	Maximum Marks
1	*Network Devices*	*10*
2	*IP Telephony*	*20*
3	*Wi-Fi*	*10*
4	*Software Defined Network (SDN)*	*10*
5	*Network Access Control (NAC)*	*15*
6	*AD, DNS, DHCP etc.*	*10*
7	*Network Security solution*	*15*
8	*Solution for Virtual Private Network (VPN)*	*10*
9	*Video conferencing solution*	*10*

10	*Patch Management solution*	*10*
	Total	**120**

B. Bidder Capability including Proven Relevant Experience (80 marks)

i. Past projects:

Bidder should have experience in implementing and managing project preferably in a Regulatory Body/Govt./any other organization of comparable nature and complexity of the projects. As part of the technical bid evaluation, bidder is required to submit at least two customer references of which at least one project should have been completed. Bidders need to submit copy of work order, completion certificate or extract from the contract mentioning the scope of work and list of technologies used. Bidders are required to submit only those client references where list of technology stack implemented is similar to the proposed solution.

Bidder shall take necessary approval from the customers for the site visits of SEBI's Tender Evaluation Committee. SEBI shall visit at least one customer's site towards the evaluation.

ii. Professional capabilities[5]:

The Bidder is required to propose the Project Team for complete execution of the project along with their CV's. Bidder shall provide the same team members including members of subcontractor, if applicable, whose CVs have been submitted in the Technical Bid. SEBI reserves the right to interview the candidate before indicting him/her in the project.

iii. Evaluation criteria[6]:

Table 9: Bidder Capability including Proven Relevant Experience

Sr. No.	**Evaluation Criteria**	**Total Marks**
1	**Customer references (minimum Two References) should include:** (20 marks per project)	40
a.	**Similarity of Technology Stack** – Similar Technology stack (SDN or NAC plus at least 5 technologies) as proposed to SEBI: 4 Similar Technology stack (SDN or NAC plus at least 3 technologies) as proposed to SEBI: 2 Totally different technology stack: 0	8

---

[5] In case Bidder proposes subcontracting for all or part of services offered for this project, the relevant experience of the subcontractor along with professional capabilities of its project team will also be evaluated

[6] Marks will be given subject to client validation

b.	**Span of the Solution –** At least 1 project involving multiple technologies (>=8) & multiple offices (>10 offices in different states) :4 Other Project: >=5 Technologies & >=5 Offices in different states :2 >=2 Technologies & >=2 Offices in different states:1 1 or less Technology and Office: 0			8
c.	Nature of project (at least one implementation project is required)– Implementation & Support: 4 Only Implementation: 2 Only Support: 1			8
d.	Status of the project – Completed: 2 Under implementation: 1 Delayed: 0			8
e.	Manpower deployed – Similar to proposed in SEBI: 2 Non similar : 0			4
f.	DC & DR implementation (marks obtained here are per project) – Yes: 2 No : 0			4
2	Customer Site visit/ Video Conference (Feedback received from selected client broadly on the above-mentioned criterion)			20
3	Proposed Project Team and their CVs (Form 7 & 8)			20
		With relevant Experience	With Certification	
a.	Project Manager	2	2	4
b.	Solution Architect	3	2	5
c.	Technology Expert	2	2	4
d.	Support Engineers (L1)	2	2	4
e.	Security Expert	1	2	3
	Total			80

C. Understanding of SEBI's requirement and Presentation to TEC (100 marks)

Table 10: Understanding of SEBI's requirement and Presentation to TEC

SN	Evaluation Criteria	Total Marks
1	Solution proposed by Bidder (refer to Form 5)	40
2	Technical Presentation to Bid Evaluation Committee	60
	Total	**100**

D. Proof of Concept (80 marks)

i. As part of the evaluation process, the bidders will be required to demonstrate Proof of Concept (POC). POC testing should be carried out by bidder in conjunction with Tender Evaluation Committee (TEC) and SEBI officials as part of the POC. The system used for POC should be identical to the solution proposed by the Bidder. The Bidder is required to select the make/model specifications as proposed in the Bidder's solution. The cost of conducting the POC shall be borne by the Bidder. However, SEBI will bear the cost of travel, lodging and boarding for the Tender Evaluation Committee (TEC) and the SEBI officials accompanying the TEC.

ii. The Bidder is requested to host the evaluation of the POC and the product walk-through at the bidder/OEM's own development centre. **The evaluation and the walk through are expected to be for 1 working day (One day for PoC per bidder)**. The bidder is expected to have all subject matter experts available to respond to SEBI queries promptly. SEBI will be in contact with each bidder to finalise the dates of the evaluation and walk through. **The POC should be completed within 45 days of opening of Technical bid**.

The Bidder will have to demonstrate Integrated Proof of Concept (PoC) as part of technical evaluation based on the following method:

Table 11: Break up of Technology wise PoC Marks

SN	Evaluation Criteria	Total Marks
1	Validation of Mandatory Product Features (Refer Appendix VI) for all solutions under clause 2.3 and/or during evaluation process /PoC	
2	Undertaking POC with Test Cases for the following technologies	80
	i. SDN	20

	ii.	NAC	20
	iii.	Wi-Fi	20
	iv.	VPN/Work From Home	20

Proof of concept for following technologies but not limited to may be demonstrated-

i. Proof of Concept (POC) for NAC solution
ii. Proof of Concept (POC) for SDN solution
iii. Proof of Concept (POC) for WI - Fi solution
iv. Proof of Concept (POC) for VPN/Work From Home solution

iii. **PoC Environment:** Bidder are required to show a representative 3-tier topology comprising of below mentioned Network devices/solutions-

i. Access Switch
ii. Core Switch
iii. Server Farm Switch
iv. Wireless Controller and Access Points
v. NAC
vi. VPN/Work From Home
vii. Firewall

iv. **PoC Test cases and Marking:** Bidders are required to demonstrate the following test cases-

a. **PoC test cases for SDN solution: (Total Marks-15)**

i. **Automation: (On 1 Network switch (L2) and 1 Firewall): (4.5 Marks)**

  a. Bidder has to demonstrate automation of Zero Touch Provisioning and configuration of network devices using Templates/ Network profiles.

  b. **Software Upgrade Life-Cycle Management:** Bidder has to demonstrate minimum one patch upgrade including Pre and Post upgrade checks such as Flash drives space availability.

ii. **Assurance: (3 Marks)**

  a. **Configuration compliance:** Bidder has to demonstrate comparison of two versions of network device configuration-
    1. For Wi-Fi controller
    2. For Network switches (Network switch L2)

iii. **Troubleshooting: Health Dashboard (Out of Box capabilities only) (6 Marks)**
    a. Bidder has to demonstrate display of network devices showing their health status.
    b. Top 10 network related issues with categorization of issues as per priority.
    c. Bidder has to demonstrate display of Health score of network devices.
    d. Bidder has to demonstrate online status change of devices.

iv. **Proactive Wireless Troubleshooting: (1.5 Marks)**
    a. Bidder has to demonstrate proactive sensor based tests for DNS and DHCP connectivity.

b. **Proof of Concept test cases for NAC solution: (Total Marks-15)**

i. **Authentication (4.5 Marks):** Bidder has to demonstrate authentication and authorization using Active directory solution having multiple user groups (at least three during PoC).

ii. **Profiling (3 Marks):** Bidder has to demonstrate End point detection and profiling for end-point devices i.e. 1 desktop, 1 IP Phone and 1 Wireless mobile.

iii. **Posturing (3 Marks):** Bidder has to demonstrate verification of End point device posture based upon OS patch, Antivirus version, Registry keys.

iv. **Guest User Access Management (4.5 Marks):** Bidder has to demonstrate functionality to self-service device on-boarding to enable secure network access.

c. **Proof of Concept test cases for Wi - Fi solution: (Total Marks-15)**

i. **Geo restricted Access: (4.5 Marks)**
Bidder has to demonstrate that only specific users should be allowed to access Wi-Fi in a particular area in the campus demarcated for specific users.

ii. **Pro Active troubleshooting: (6 Marks)**
Bidder has to demonstrate troubleshooting using wireless sensors.
    a. Bidder has to demonstrate proactive Wi-Fi troubleshooting using Wi-Fi sensors.

b. Bidder should demonstrate test scenario for reachability and performance of DNS server, DHCP server and radius server, etc.

iii. **Rogue AP Detection: (4.5 Marks)**

a. Bidder has to demonstrate identification of any AP which is not sanctioned/authorized by local network administrator.

b. Bidder has to demonstrate solution to show access points deployed across campus and track rogue access points and Wi-Fi interferers.

d. **Proof of Concept test cases for VPN solution/Work From Home: (Total Marks-15)**

i. **Authentication: (4.5 Marks)**

a. Bidder has to demonstrate secure authentication including 2FA and captcha.

ii. Security Check/Profiling: (6 Marks)

Bidder has to demonstrate verification of End point device posture based upon OS patch, Antivirus version.

iii. Split Tunneling: (4.5 Marks)

Bidder has to demonstrate Split tunneling functionality where only specific traffic must be tunneled.

e. **One use case showing above 4 technologies in an integrated scenario –**

i. On boarding of laptop on SEBI Wi – Fi **(10 Marks)**
ii. On boarding of laptop through VPN **(10 Marks)**

E. Training (20 marks)

Bidders are required to impart preferably OEM based training for all the key technologies as proposed in solution design. OEM classroom training with Certification coupon to at least 5 SEBI officers. Participant would be required to take a certificate test at their own cost utilising the coupon provided during the training. OEM certification should be as per industry standards and related to the solution proposed by the bidder.

Scoring based on Appendix I Form 17: OEM Training Details

Technical evaluation based on the following method:

Table 12: List of Technologies for Training

Sr. No.	List of Key Technologies	OEM-Classroom	OEM-Online	Non-OEM Classroom	Coupon	Total
1	NAC	2.0	0.5	1		3.5
2	Network Devices and Network Security solution	2.0	0.5	1		3.5
3	Software Defined Network	2.0	0.5	1		3.5
4	AD, DNS, DHCP	2.5	0.5	1		4.0
5	Video Conferencing	0	0	1		1.0
6	Others	0.5	0.5	0.5		1.5
7	OEM Certification/coupon				3.0	3.0
	Total					**20**

3.3. Commercial Bid Evaluation

a. The Commercial Bids of technically qualified Bidders i.e., Bidders scoring more than 75% marks overall and more than 65% marks in individual evaluation criteria, will be opened on the prescribed date in the presence of Bidder representatives.

b. The commercial bids will be evaluated on the basis of Total Cost of Ownership (TCO) over a seven and half year period converted to Net Present Value (NPV) calculated using a nominal interest rate of 8 % per annum for second and subsequent years of the duration. AMC charges for 4 years will be considered for calculating the NPV. The bidder with the lowest NPV, termed L1 bidder, shall qualify for the award of contract.

c. Only fixed price financial bids indicating total price for all the deliverables and services specified in this bid document will be considered.

d. The bid price shall be in Indian Rupees. The bid price shall be firm and exclude taxes and levies.

e. Any conditional bid would be rejected.

f. Errors & Rectification: Arithmetical errors will be rectified on the following basis: “If there is a discrepancy between the unit price and the total price that is obtained by multiplying the unit price and quantity, the unit price shall prevail and the total price shall be corrected. If there is a discrepancy between words and figures, the amount in words will prevail”.

4. Conditions Specific to SIT-NET Project

4.1. Acceptance of Project

4.1.1. Acceptance Testing Criteria

Solution would be deemed accepted based on the completion of the following requirements and accordingly Go-live would be recommended–

a) Completion and submission of UAT report for all the proposed solutions including Migration completeness testing.
b) Implementation of DR plan with reference to clause 2.2.5.
c) Compliance to zero trust model with reference to clause 2.2.6.b.
d) Completion and submission of VAPT observations and rectification of VAPT observations with reference to clause 2.2.13.
e) Submission of Technical Documentations with reference to clause 4.1.2.b

4.1.2. Quality Assurance (QA) Testing and User Acceptance Tests (UAT) Activities

a. QA test of the SIT-NET shall be completed by the Bidder and results of the same shall be shared with SEBI as specified in the accepted solution design by SEBI.

b. The User Acceptance Tests (and repeats of such tests) shall be conducted by SEBI in coordination with the Bidder during Commissioning of the SIT-NET, to ascertain whether the SIT-NET conforms to the Technical Requirements and meets SEBI's performance requirements, including, but not restricted to, scope of work defined under clause 2.2 and the functional and technical performance requirements defined under clause 2.3. The User Acceptance Tests shall be conducted in accordance with the test scripts/programs approved by SEBI.

c. UAT would be conducted for individual technologies and also as part of overall integration testing including migrated data as per clause 2.2.14.

d. SEBI shall issue a User Acceptance Certificate after successful completion of UAT.

e. SEBI shall also notify the bidder in writing of any defect for deficiencies or other reason for the failure of the UAT, if any.

f. The Bidder shall use all reasonable endeavors to promptly remedy any defect and/or deficiencies and/or other reasons for the failure of the User Acceptance Test that SEBI has notified the Bidder. Once the Bidder has made such remedies, it shall notify SEBI, and SEBI, with full cooperation of the Bidder, shall use all reasonable endeavors to promptly carry out retesting of the System. Upon the successful conclusion of the User Acceptance Tests including successfully complying all integration touch points, SEBI shall issue the User Acceptance Certification in accordance with RFP. The procedure set out in this RFP shall be repeated, as necessary, until a User Acceptance Certificate is issued.

4.1.3. Technical Documentation

a. Documentation for software components:

The Bidder shall deliver all the relevant documents to SEBI for all software components including third party software before the SIT-NET is declared Go-live , which may include, but not limited to user manuals, installation manuals, operation manuals, design documents, process documents, technical manuals, functional specifications, on-line tutorials, system configuration documents, system administrative documents, debugging/diagnostics documents, test procedures etc.

b. Documentation for solution:

Bidder shall deliver all relevant documentation pertaining to solution in the appropriate format. The indicative list may include but not limited to-

i. Business Requirement Documents
ii. Installation Documents
iii. Functional/System Requirement Specification Documents
iv. Design documents
v. Solution wise Architecture/Architecture Documents / Network Diagram/ high level design doc/ low level design documents
vi. Risks and Mitigation Documents
vii. Gap analysis Documents
viii. Project Plan
ix. Project Management Reports (On weekly basis)
x. Test Plans
xi. Comprehensive UAT Test Cases Document (Unit, Integration and SIT Test Cases)
xii. Security Management Guide
xiii. User Management Guide
xiv. Production Deployment Plan
xv. Solution Configuration Documents
xvi. Operational Manual
xvii. Operational Acceptance Checklist
xviii. DR-BCP Strategy and procedures
xix. Backup Strategy and procedures

4.1.4. Go-Live

Production use (Go Live) shall commence only after meeting the acceptance testing criteria mentioned under clause 4.1.1. Subsequently the project would be under stabilisation phase where for at least one month, the SIT-NET solution should run in a satisfactory manner.

4.2. Implementation Schedule

The bidders are required to adhere to the following proposed timelines

Table 13: Project Implementation Timelines

Sr. No.	**Component**	**Duration From Date of Agreement**
_1_	Delivery of Infrastructure Components including equipment (Hardware, Software, Licenses etc.)	_8 weeks_
_2_	Implementation and UAT	_18 weeks_
_3_	Risk Assessment, Mitigation and Audit	_22 weeks_
_4_	Stabilisation	_26 weeks_
_5_	Go Live	_26 weeks_
_6_	Training	_As per SEBI's Training schedule_

4.3. Payment Schedule

Unless otherwise stated the general terms of payment are:
50 % of the Component value on Delivery
40 % of the Component value on Installation & Acceptance
10% of the Component value on Go-Live

4.3.1. The payment schedule is delivery based and segregated for the following technology solutions.

i. Network Devices
ii. IP Telephony
iii. Wi-Fi
iv. Software Defined Network (SDN)
v. Network Access Control (NAC)
vi. AD, DNS, DHCP etc.
vii. Network Security solution
viii. Solution for Virtual Private Network (VPN)
ix. Video conferencing solution
x. Patch Management solution

Table 14: Payment Schedule as per the milestones

SN	***Deliverables***	***Clause of Scope of Work***	***Item/ section in Bill of Material (Form 2)***	***% of Payment***	***Stages (On Completion of the Activities)***

1	For the Technology based solutions		*A*		
a.	Delivery for respective Technology solution			*50*	*On delivery and power on Test including submission of Power on Test report*
b.	Completion and Submission of UAT report	*2.3.4*		*40*	*Implementation & UAT (clause 4.1.1 and documentation (clause 4.1.2.b)*
c.	Completion of Stabilization Phase	*2.3.9*		*10*	*Submission of report on compliance to Risk Assessment and Mitigation and Audit and declaration of Go-Live*
2	Risk Assessment, Mitigation and Audit	*2.2.13*	*C*		
a.	On submission of the report			*50%*	*The payment will be made on conduction of activities under this section on half yearly basis*
b.	On acceptance of corrective actions			*50%*	
3	*FMS- Payment for Support Services Including Resource cost, SLA etc. implemented as part of the project) during Warranty & Support, and AMC*	*2.4.1 & 2.4.2,* *2.6*	*B*		*Payment will be made on quarterly basis in arrears against submission of physical invoice. The payment will begin after signoff based on the quarterly SLA reports submitted by the bidder.*
4	*Annual Maintenance contract (AMC) for the Infrastructure Component.*		*D*	-	*Payment will be made on half yearly basis in arrears against submission of physical invoice. The payment will begin after signoff based on the half yearly SLA reports submitted by the engaged bidder. Further the engaged Bidder will be required to submit copy of the*

					back-to-back agreements with respective OEMs at the start of AMC.
5	*AMC with respect to 2.2.c*	*2.2.c*	***E***		*Payment will be made on quarterly basis in arrears against submission of physical invoice. The payment will begin after signoff based on the quarterly SLA reports submitted by the engaged bidder.*
6	*Ancillary Services*		***F***	***90***	*On delivery and implementation*
				10	*On declaration of Go-live*
7	*Training*	*2.9* *3.2.1.E*	***G***	*100% of total training cost*	*On actual basis after the completion of respective proposed trainings.*

4.4. Delays in the Bidder's Performance

The Bidder must strictly adhere to the implementation schedule, as specified in the agreement in the performance of the obligations and any delay in this regard will enable SEBI to resort to any or both of the following:

a. Claiming Liquidated Damages
b. Termination of the agreement/contract fully or partly.

4.5. Liquidated Damages

Time is the essence of this project. The Bidder shall be liable to pay SEBI liquidated damages (LD) for delay in deliveries as specified in the delivery schedule mentioned in section 4.2.

a. Bidder shall have to pay liquidated damages to SEBI at the rate of *1 (one)* percent per week on unexecuted value excluding tax of the deliverable per week or part thereof, for late delivery beyond the delivery period. There shall be an upper ceiling of *10 (ten) percent* of the Total Project Cost except the AMC cost for the Liquidated damages to be deducted under this section. The liquidated damages as applicable shall be deducted from the payment amount payable to bidder. The performance bank guarantee shall be *10 (ten) percent* of the order value irrespective of the penalties levied.
b. In case of shortfall in the uptime / SLA, etc. the payment shall be adjusted as per the credits specified in SLA clause.

c. The Bidder agrees and considers that the liquidated damages set out herein above are fair and reasonable and that he will raise no objection or dispute with regard to SEBI's right to recover the liquidated damages.
d. Liquidated Damage is not applicable for the reasons attributable to SEBI and Force Majeure.
e. SEBI will have the rights to recover the liquidated damages, if any, from any amount payable to the Bidder. Also, if the specifications of the RFP are not met by the Bidder during various tests, the Bidder shall rectify or replace the same to comply with the specifications immediately to ensure the committed uptime, failing which SEBI has the sole right either to reject or to accept it finally by recovering the suitable amount as deemed reasonable by SEBI.
f. SEBI may without prejudice to its right to effect recovery by any other method, deduct the amount of liquidated damages from any money belonging to the Bidder in its hands (which includes the SEBI's right to claim such amount against Bidder's performance Guarantee / security) or which may become due to the Bidder. Any such recovery or liquidated damages shall not in any way relieve the Bidder from any of its obligations to complete the works/services or from any other obligations and liabilities under the Agreement.

4.6. Service Level Agreement

a. SLAs define the quality and timeliness of service delivery during the course of the project. They help SEBI sustain the planned business outcomes from the solution deployed on a continued basis over a sustained period of time.
b. The Bidder need to execute a Service Level Agreement with SEBI covering all terms and conditions of this tender. Bidder need to strictly adhere to Service Level Agreements (SLA). SEBI shall without prejudice to its other rights and remedies under and in accordance with the terms of the RFP levy liquidated damages in case of breach of SLA by the bidder. Services delivered by bidder should comply with the SLA mentioned in Appendix X - Annexure B.
c. Service Levels will include Availability measurements and Performance parameters.
d. The Bidder shall provide Availability Report on monthly basis and a review shall be conducted on quarterly basis.
e. Bidder shall use an appropriate tool for the purpose of such reporting.
f. Performance measurements would be assessed through audits or reports, as appropriate to be provided by the Bidder e.g. utilization reports, response time measurement reports, etc. The tools to perform the audit will need to be provided by the Bidder. The specification for audit are as per the functional and technical requirements at Scope of work and Appendix VI.
g. All the components of the SIT-NET Infrastructure should be of commercially licensed version with unlimited incident support with L1, L2, L3 level technical support (Email, Web & Telephonic) directly from original OEM. The support should be available 24x7x365 with unlimited software updates and upgrades during the complete tenure of the agreement without any additional cost, during the validity of the agreement.

h. **System availability/System Uptime is defined as:**
{(Scheduled operation time – system downtime) / (scheduled operation time)} * 100%

i. Scheduled operation time means the scheduled operating hours of the System for the month. All planned downtime (for system maintenance) on the system would be deducted from the total operation time for the month to give the scheduled operation time.

j. System downtime subject to the SLA, means accumulated time during which the System is not available to SEBI's users or customers due to in-scope system or infrastructure failure, and measured from the time SEBI and/or its customers log a call with the Bidder help desk of the failure or the failure is known to the Bidder from the availability measurement tools to the time when the System is returned to proper operation. Ideally system failure or outages should be captured by audit tools of the system.

k. The selected Bidder will be required to schedule 'planned maintenance time' with prior approval of SEBI. This will be planned outside working hours. In exceptional circumstances, SEBI may allow the Bidder to plan scheduled downtime in the working hours where actual production downtime will be minimal.

l. SEBI's technology operation hours are 24*7*365. SEBI's business hours are typically between 8 am to 10 pm (Monday to Friday) and the SLA will be applicable according to the technological operations window i.e. 24*7*365.

m. The Bidder shall make sure that the infrastructure and all deployed solutions and components are available to SEBI in proper working condition in fully configured state as per the respective uptime requirements.

n. Uptime is defined as the uptime of the SIT-NET solution components such as servers, node, storage, VM, Security Components like Firewall etc. If any significant part of the solution or cluster is unavailable or inaccessible or unresponsive to end users, it will be considered down-time. SEBI's decision will be final in determining downtime.

o. SLA Holiday: The SLA holiday period of not more than a quarter would be provided to the bidder post Go-Live date. This SLA holiday period is only for the purpose of streamlining the SLA measurement and monitoring process of the *SIT-NET* Project. The SLAs will be reviewed by SEBI during SLA Holiday period and finalized for operations.

p. Commencement of SLA: The SLA shall commence after Go-Live has been declared. The liquidated damages will be deducted from the next payment milestone after the SLA holiday period.

q. The total Liquidated damages deduction per quarter (for breach of SLA) shall not exceed *10 (ten) percent* of the total Quarterly Payment value.

5. Appendix I Technical Bid Templates

The Bidders are expected to respond to the RFP using the forms given in this section and all documents supporting Technical Evaluation Criteria.

Forms to be used in Technical Proposal

Form 1: Compliance Sheet for Technical bid

Form 2: Pre-Contract Integrity Pact

Form 3: Letter of Proposal

Form 4: Project Citation Format

Form 5: Proposed Solution and write up

Form 6: Proposed Work Plan

Form 7: Team Composition

Form 8: Curriculum Vitae (CV) of Key Personnel

Form 9: Details of Proposed Products /services back to back support and service agreements with OEM

Form 10: OEM Response Compliance Sheet

Form 11: Undertaking from OEM

Form 12: Bank Details

Form 13: Self Declarations

Form 14: Letter for Refund of EMD

Form 15: Consortium Details

Form 16: Letter from consortium member

Form 17: OEM Training details

Form 18: Bank Guarantee

Form 19: Masked Bill of Material (Refer to clause 6.2-Form 2 for format)

5.1. Form 1: Compliance Sheet for Technical Bid

The Technical bid should comprise of the following basic requirements. The documents mentioned in this compliance sheet along with this form, needs to be a part of the Technical bid.

SN	Specific Requirements	Documents Required	Compliance	Reference & Page Number
1	Covering Letter for Technical Proposal	As per Form 3	Yes / No	
2	Implementation and Operational Management of SIT-NET (last 5 years)	Completion Certificates from the client; OR Work Order + Self Certificate of Completion (Certified by the Statutory Auditor); OR Work Order + Phase Completion Certificate (for ongoing projects) from the client; and Project citation (Form 4)	Yes / No	
3	Solution and Technologies Proposed, Approach & Methodology (may refer to Scope of work and Deliverables), Understanding and Work Plan (refer to section 2.2, 2.3, 2.4, 2.5, 2.6, 2.7, 2.8)	A note (Form 5 & 6) The note should highlight understanding of SEBI’s requirements through providing justifications for: 1) Solution proposed and its components, 2) Technologies used, 3) Challenges likely to be encountered 4) Learning on how to deal with the challenges	Yes / No	

4	Resume of all key technical resources proposed for the assignment (Refer clause 2.4)	CV & a Note (Form 7 and 8)	Yes / No	
5	Earnest Money Deposit		Yes / No	
6	Soft Copy of Technical Bid in MS Office (Word/ Excel) or PDF format submitted		Yes / No	
7	Whether the Bid is authenticated by authorized person		Yes / No	
8	Contact person, contact number and address for the Project		Yes / No	
9	All the pages are numbered properly		Yes / No	
10	All pages are authenticated by sign and seal (Full signature to be affixed and not initials). Erasures / Overwriting / Cutting / Corrections authenticated Certification / Undertaking is authenticated.		Yes / No	
11	Whether price quoted in Bill of Material in Financial bid as per the format are exclusive of Taxes		Yes / No	
12	Whether replica of price Bid is enclosed in Technical masked bid price		Yes / No	
13	Whether Taxes and Duties are separately indicated in price bid		Yes / No	

14	Post warranty AMC for a minimum period of 4 years offered		Yes / No	
15	AMC for the existing Network Set up and Network Devices (Refer clause 2.2.c)		Yes / No	
16	Buyback proposal of equipment under existing Network project (Refer clause 2.2.d)		Yes / No	
17	Pre-Contract Integrity Pact	Form 2	Yes/ No	
18	Signed copy of RFP		Yes / No	
19	Self-Declaration	Form 13	Yes / No	

5.2. Form 2: Pre-Contract Integrity Pact

INTEGRITY PACT

Between

SECURITIES and EXCHANGE BOARD OF INDIA hereinafter referred to as "The Principal",

and

………………………………………………. Hereinafter referred to as "The Bidder/ Contractor"

Preamble

The Principal intends to award, under laid down organizational procedures, contract/s for ………………………….. The Principal values full compliance with all relevant laws of the land, rules, regulations, economic use of resources and of fairness/ transparency in its relations with its Bidder (s) and / or Contractor (s).

In order to achieve these goals, the Principal will appoint Independent External Monitors (IEMs) who will monitor the tender process and the execution of the contract for compliance with the principles mentioned above.

Section 1 – Commitments of the Principal

(1) The Principal commits itself to take all measures necessary to prevent corruption and to observe the following principles:-

  a. No employee of the Principal, personally or through family members, will in connection with the tender for, or the execution of a contract, demand, take a promise for or accept, for self or third person, any material or immaterial benefit which the person is not legally entitled to.

  b. The Principal will, during the tender process treat all Bidder(s) with equity and reason. The Principal will in particular, before and during the tender process, provide to all Bidder(s) the same information and will not provide to any Bidder(s) confidential/ additional information through which the Bidder(s) could obtain an advantage in relation to the tender process or the contract execution.

c. The Principal will exclude from the process all known prejudiced persons.

(2) If the Principal obtains information on the conduct of any of its employees which is a criminal offence under the IPC/ PC Act, or if there be a substantive suspicion in this regards, the Principal will inform the Chief Vigilance Officer and in addition can initiate disciplinary actions.

Section 2 – Commitments of the Bidder(s)/ Contractor(s)

(1) The Bidder(s) / Contractor(S) commit themselves to take all measures necessary to prevent corruption. The Bidder(s)/ Contractor(s) commit themselves to observe the following principles during participation in the tender process and during the contract execution.

a. The Bidder(s)/ Contractor(s) will not, directly or through any other person or firm, offer, promise or give to any of the Principal's employees involved in the tender process or the execution of the contract or to any third person any material or other benefit which he/ she is not legally entitled to, in order to obtain in exchange any advantage of any kind whatsoever during the tender process or during the execution of the contract.

b. The Bidder(s)/ Contractor(s) will not enter with other Bidder into any undisclosed agreement or understanding, whether formal or informal. This applies in particular in prices, specifications, certifications, subsidiary contracts, submission or non- submission of bids or any other actions to restrict competitiveness or to introduce cartelization in the bidding process.

c. The Bidder(s)/ Contractor(s) will not commit any offence under the relevant purposes of competition or personal gain, or pass on to others, any information or document provided by the Principal as part of the business relationship, regarding plans, technical proposals and business details, including information contained or transmitted electronically.

d. The Bidder(s)/ Contractor(s) of foreign origin shall disclose the name and address of the Agents/ representatives in India, if any. Similarly the Bidder(s)/ Contractor(s) of Indian Nationality shall furnish the name and address of the foreign principals, if any.

e. The Bidder(s)/ Contractor(s) will, when presenting their bid, disclose any and all payments made, is committed to or intends to make to agents, brokers or any other intermediaries in connection with the award of the contract.

(2) The Bidder(s) / Contractor(s) will not instigate third persons to commit offences outlined above or be an accessory to such offences.

Section 3 – Disqualification from tender process and exclusion from future contracts

If the Bidder(s)/ Contractor(s), before award or during execution has committed a transgression through a violation of Section 2, above or in any other form such as to put their reliability or credibility in question, the Principal is entitled to disqualify the Bidder(s)/ Contractor(s) from the tender process.

Section 4 – Compensation for Damages

(1) If the Principal has disqualified the Bidder(s) from the tender process prior to the award according to Section 3, the Principal is entitled to demand and recover the damages equivalent to Earnest Money Deposit/ Bid Security.

(2) If the Principal has terminated the contract according to Section 3, or if the Principal is entitled to terminate the contract according to Section 3, the Principal shall be entitled to demand and recover from the Contractor liquidated damages of the Contract value or the amount equivalent to Performance Bank Guarantee.

Section 5 – Previous transgression

(1) The Bidder declares that no previous transgressions occurred in the last three years with any other Company in any country conforming to the any – corruption approach or with any Public Sector Enterprise in India that could justify his exclusion from the tender process.

(2) If the Bidder makes incorrect statement on this subject, he can be disqualified from the tender process or *the contract, if already awarded, can be terminated for such reason*.

Section 6 – Equal treatment of all Bidders/Contractors/Subcontractors

(1) In case of Sub-contracting, the Principal Contractor shall take the responsibility of the adoption of Integrity Pact by the Sub –contractor.

(2) The Principal will enter into agreements with identical conditions as this one with all Bidders and Contractors.

(3) The Principal will disqualify from the tender process all bidders who do not sign this Pact or violate its provisions.

Section 7 – Criminal charges against violating Bidder(s)/Contractor(s)/ Sub-Contractor(s)

If the Principal obtains knowledge of conduct of a Bidder, Contractor or Sub-contractor, or of an employee or a representative or an associate, of a Bidder, Contractor or Sub-contractor which constitutes corruption, or if the Principal has substantive suspicion in this regard, the Principal will inform the same to the Chief Vigilance Officer.

Section 8 – Independent External Monitor

(1) The Principal appoints competent and credible Independent External Monitor for this Pact after approval by Central Vigilance Commission. The task of the Monitor is to review independently and objectively, whether and to what extent the parties comply with the obligations under this agreement.

(2) The Monitor is not subject to instructions by the representatives of the parties and performs his/ her functions neutrally and independently. The Monitor would have access to all Contract documents, whenever required. It will be obligatory for him/ her to treat the information and documents of the Bidders/ Contractors as confidential. He/ she reports to the Chairman, *SEBI.*

(3) The Bidder(s)/ Contractor(s) accepts that the Monitor has the right to access without restriction to all Project documentation of the Principal including that provided by the Contractor. The Contractor will also grant the Monitor, upon his/ her request and demonstration of a valid interest, unrestricted and unconditional access to their project documentation. The same is applicable to Sub-contractors.

(4) The Monitor is under contractual obligation to treat the information and documents of the Bidder(s)/ Contractor(s)/ Sub-contractor(s) with confidentiality. The Monitor has also signed declarations on “Non- Disclosure of Confidential Information” and of “Absence of Conflict of Interest”. In case of any conflict of interest arising at a later date, the IEM shall inform Chairman, SEBI and recuse himself/ herself from that case.

(5) The Principal will provide to the Monitor sufficient information about all meetings among the parties related to the Project provided such meetings could have an impact on the contractual relations between the Principal and the Contractor. The parties offer to the Monitor the option to participate in such meetings.

(6) As soon as the Monitor notices, or believes to notice, a violation of this agreement, he/ she will so inform the Management of the Principal and request the Management to discontinue or take corrective action, or to take other relevant action. The monitor can in this regard submit non-binding recommendations.

Beyond this, the Monitor has no right to demand from the parties that they act in a specific manner, refrain from action or tolerate action.

(7) The Monitor will submit a written report to the Chairman, SEBI within 8 to 10 weeks from the date of reference or intimation to him by the Principal and, should the occasion arise, submit proposals for correcting problematic situations.

(8) If the Monitor has reported to the Chairman, SEBI, a substantial suspicion of an offence under relevant IPC/ PC Act, and the Chairman, SEBI has not within the reasonable time taken visible action to proceed against such offence or reported it to the Chief Vigilance Officer, the Monitor may also transmit this information directly to the Central Vigilance Commissioner.

(9) The word "**Monitor**" would include both singular and plural.

Section 9 – Pact Duration

This Pact begins when both parties have legally signed it. It expires for the Contractor 12 months after the last payment under the contract, and for all other Bidders 6 months after the contract has been awarded. Any violation of the same would entail disqualification of the bidders and exclusion from future business dealings.

If any claim is made/ lodged during this time, the same shall be binding and continue to be valid despite the lapse of this pact as specified above, unless it is discharged/ determined by Chairman of SEBI.

Section 10 – Other Provisions

(1) This agreement is subject to India Law. Place of performance and jurisdiction is the *Registered Office of the Principal, i.e. Mumbai*.

(2) Changes and supplements as well as termination notices need to be made in writing. Side agreements have not been made.

(3) If the Contractor is a partnership or a consortium, this agreement must be signed by all partners or consortium members.

(4) Should one or several provisions of this agreement turn out to be invalid, the remainder of this agreement remains valid. In this case, the parties will strive to come to an agreement to their original intentions.

(5) Issues like Warranty/ Guarantee etc. shall be outside the purview of IEMs.

(6) In the event of any contradiction between the Integrity Pact and its Annexure, the Clause in the Integrity Pact will prevail.

________________________ ______________________

(For & On behalf of the Principal) (For & On behalf of Bidder/ Contractor)

(Office Seal) (Office Seal)

Place: __________

Date: __________

Witness 1:

(Name & Address) _______________________
____
____
____

Witness 2:

(Name & Address) _______________________
____
____
____

5.3. Form 3: Letter of Proposal

To:

Chief General Manager – ITD
Securities and Exchange Board of India
SEBI Bhavan,
Plot No. C4-A, “G Block”
Bandra Kurla Complex
Bandra (East) - 400 051
India

Subject: Submission of the Technical bid for SIT-NET

Dear Sir/Madam,

We, the undersigned, offer to provide Implementation Services to SEBI for “SIT-NET” with your Request for Proposal <*RFP NO*> dated <*Date of RFP*> and our Proposal. We are hereby submitting our Proposal, which includes this Technical bid and the Financial Bid sealed.

We hereby declare that all the information and statements made in this Technical bid are true and accept that any misinterpretation contained in it may lead to our disqualification.

We undertake, if our Bid is accepted, to initiate the Implementation services related to the assignment not later than the date indicated in the RFP.

We agree to abide by all the terms and conditions of the RFP document. We would hold the terms of our bid valid for *120 days* as stipulated in the RFP document.

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

Yours sincerely,

Authorized Signature [*In full and initials*]:

Name and Title of Signatory:

Name of Firm:

Address:

Location: Date:

5.4. Form 4: Project Citation Format

Sl. No.	**RELEVANT PROJECT EXPERIENCE (PROVIDE NO MORE THAN 5 PROJECTS IN THE LAST 5 YEARS)**	
1	**General Information**	
i.	Name of the project	
ii.	Client for which the project was executed	
iii.	Name and contact details of the client	
2	**Project Details**	
i.	Description of the project	
ii.	Scope of services	
iii.	Technologies and solutions implemented	
iv.	Status of the project (Completed/On-going/Warranty/AMC)	
v.	Duration of the project (no. of months, start date, completion date, current status)	
3	**Other Details**	
i.	Total cost of the project (indicative/approximate)	
ii.	Total cost of the services (indicative/approximate)	
iii.	Total Manpower (No. of L1,L2,L3 etc.) deployed	
4	**Other Relevant Information**	

i.	Letter from the client to indicate the successful completion of the projects	
ii.	Copy of Work Order	

5.5. Form 5: Proposed Solution and Write Up

i. Technical approach, methodology and work plan are key components of the Technical Proposal. Bidders are suggested to present Approach and Methodology for implementing the Scope of Work divided into the following sections:

Table 15: Key features of the proposed solution

Sr. No.	Scope of Work	Reference clause
1	Overall SIT-NET architecture	2.2.1
2	Capacity and Sizing	2.2.2
3	Project Management, Implementation Methodology and Timeline	2.2.4
4	Business Continuity and Disaster Recovery	2.2.5
5	Network and Security	2.2.6
6	Performance Monitoring and MIS Reports	2.2.7
7	Standards: Compatibility and Interoperability	2.2.8
8	Maintenance and Support	2.2.9
9	Versions, Upgrades and Updates	2.2.10
10	Licenses	2.2.11
11	Risk Assessment, Mitigation and Audit	2.2.13
12	Migration Plan	2.2.14

ii. Integration approach with other IT Infrastructures of SEBI.

5.6. Form 6: Proposed Work Plan

The proposed work plan should be in accordance to the clause of Deliverable and Timeline as mentioned in the Section 4.2.

5.7. Form 7: Team Composition

Sl. No.	Name of staff with qualification and experience	Year of joining the organisation	Area of Expertise	Position Assigned	Task Assigned	Time committed for the engagement (Full time/Part time) in Hours	Key personnel (Yes/No)

5.8. Form 8: Curriculum Vitae (CV) of Key Personnel

CV of all the following Key Personnel should be submitted.

Table 16: CV types

Sr. No.	Key Personnel Role	Type of CV
1	Project Manager	Named resource
2	Technology Expert	Named resource
3	Solution Architect	Named resource
4	Security Expert	Named resource
5	Team Members	Indicative CV. Named resources CV will be submitted at the time of implementation for selection by SEBI.

The submitted CV should be in the following format:

1	Name of the person	
2	Current Designation / Job Title	
3	Current job responsibilities	
4	Proposed Role in the Project	
5	Proposed Responsibilities in the Project	
6	Academic Qualifications:	
	i. Degree	
	ii. Academic institution graduated from	
	iii. Year of graduation	
	iv. Specialization (if any)	
	v. Key achievements and other relevant information (if any)	
7	Professional Certifications (if any)	
8	Total number of years of experience	
9	Number of years with the current company	
10	Summary of the Professional / Domain Experience	
11	Number of complete life cycle implementations carried out	
12	The names of customers (Please provide the relevant names)	
13	Past assignment details (For each assignment provide details regarding name of organizations worked for, designation, responsibilities, tenure)	
14	Prior Professional Experience covering:	
	a. Organizations worked for in the past	
	i. Organization name	
	ii. Duration and dates of entry and exit	
	iii. Designation Location(s)	
	iv. Key responsibilities	
	b. Prior project experience	
	i. Project name	
	ii. Client	

	iii. Key project features in brief	
	iv. Location of the project	
	v. Designation	
	vi. Role	
	vii. Responsibilities and activities	
	viii. Duration of the project	
15	Please provide only relevant projects.	

5.9. Form 9: Details of Proposed Products/Services Back to Back Support and Service Agreements with OEM

Bidder should provide the level of support and back to back support/service agreement details with respective OEM's for the proposed project components as per the below format. The bidder should provide details for all the products/services quoted as part of this project in the following format (please see next page).

Sl. No.	Proposed product/ service name	Product model and version	Name of Product/ service OEM	Whether free software updates and free upgrades covered under OEM back to back support agreement for entire duration of Agreement?	Whether Back to back support agreement exists with OEM for entire duration of Agreement	Mention the product/service support level agreement with OEM for entire duration of Agreement	Whether the products/service covered under 24x7x365 back to back support from OEM? for entire duration of Agreement (if not please mention)	Hardware Replacement time (in hours) if failed, under the support agreement (in hours) for entire duration of Agreement
1								

Format for Form 9

5.10. Form 10: OEM Response Compliance Sheet

Sl. No	**Information Required**	**Response from Product OEM1**	**Response from Product OEM2**	**Response from Product OEM…N**
1	Name of OEM			
2	Name of the product			
3	Product Category			
4	Product Name			
5	Product Version			
6	Date of Release of the Version			
7	End of sale			
8	End of support			
9	Support for IPV6 (Yes/No)			
10	Road Map of product			
11	Number of certified engineers giving technical support for the product in India			
12	Specifications, attached separately (Yes/No)			
13	Address in India & Date of Incorporation in India			
14	Communication Details of Contact Official(s) – Name, Designation, Phone and email id			

5.11. Form 11: Undertaking from OEM

Response from OEM through Bidder
[On the Letter head of the OEM]
To,
Chief General Manager – ITD
Securities and Exchange Board of India
SEBI Bhavan,
Plot No. C4-A, “G Block”
Bandra Kurla Complex
Bandra (East) - 400 051
India

Ref: Authorization letter from OEM to ----- (Bidder) for participation in bid for SEBI RFP SIT-NET.

Dear Sir,

We_______ (OEM Vendor) who are established and reputed Manufacturers for____having factories/ depot at ______ and we do hereby authorize M/s.______ (Successful Bidder / Vendor Name) to offer their quotation, negotiate and conclude the contract with you against the above invitation for the Bid.
We hereby extend our full guarantee and comprehensive warranty as per terms and conditions of the tender and the contract for our equipment quoted/ services offered against this invitation for Bid by the above firm.
We undertake to perform the obligations as set out in the RFP in respect of such services as mentioned in clause “scope of work for OEM” and hereby extend our warranty / support and services through M/s.………………during the … years contract period as per terms and conditions of the RFP.
We also undertake that we have not been blacklisted by the Government Authority or Public Sector Undertaking (PSUs) in India or any Financial Institution in India as on date of submission of response.

We assure you that in the event of M/s ……………………… not being able to fulfil its obligation as M/s ……………………… Bidder in respect of the terms defined in the RFP,…………………………………… (OEM Name) would continue to meet these either directly or through alternate arrangements without any additional cost to SEBI.
The quoted product is of latest model /version and extend our back to back support during entire duration of Agreement. If any product found to be obsolete /end of support/end of life during the contract period, we will replace the same with the latest product with the equivalent /higher capabilities for free of cost.
Dated at ______________ this ________ day of _____________<*YEAR*>.

5.12. Form 12: Bank Details

(to be included in Technical Bid Envelope)

Bidder is advised to provide bank details to facilitate easy and timely credit of payments for goods delivered / services rendered.

1	Name of the Bank	
2	Address of the Bank with Contact details (name, telephone, mobile, email, etc.)	
3	Account Type	
4	Account Title	
5	Account Number	
6	IFSC Code	
7	Remarks, if any	

Signature:
Name of the Authorized Person:
Designation:
Company Seal

5.13. Form 13: Self Declarations

(Undertaking to be submitted on Bidder Company’s Letter Head)

To,
Chief General Manager – ITD
Securities and Exchange Board of India
SEBI Bhavan,
Plot No. C4-A, “G Block”
Bandra Kurla Complex
Bandra (East) - 400 051
India

Ref: RFP for SIT-NET.

We, (name and designation) on behalf of ---------having its registered office at ------- have submitted a Bid proposal to SEBI for ---------------- in response to the Request for Proposal (RFP) dated issued________by SEBI.

We are duly authorized persons to submit this undertaking.

We have read and understood the aforesaid RFP and we hereby convey our absolute and unconditional acceptance to the aforesaid RFP.

We have submitted our Bid in compliance with the specific requirements as mentioned in this RFP.

We have completed the site survey before submitting the tender in compliance with clause 2.2.12.

We have provided with all necessary information, supporting documents which are true and accurate and shall provide with such additional information’s may be required by SEBI from time to time.

Neither we nor any of our employee/director has been barred from providing the Services nor are we in negative list/blacklisted by any public sector Banks, statutory or regulatory or investigative agencies in India or abroad in the last 5 years.

All the information furnished here in and as per the document submitted is true and accurate and nothing has been concealed or tampered with. We have gone through all the conditions of Bid and are aware that we would be liable to any punitive action in case of furnishing of false information / documents.

We also undertake that, we were/are never involved in any legal case that may affect the solvency / existence of our organization or in any other way that may affect capability to provide / continue the services to SEBI.

It is further certified that we have not modified or deleted any text/matter in this RFP.
I have read the clause 1.8.18 regarding restrictions on procurement from a bidder of a country which shares a land border with India and on sub-contracting to contractors from such countries; I certify that this bidder is not from such a country or, if from such a country, has been registered with the Competent Authority and will not sub-contract any work to a contractor from such countries unless such contractor is registered with the Competent Authority. I hereby certify that this bidder fulfils all requirements in this regard and is eligible to be considered. [Where applicable, evidence of valid registration by the Competent Authority shall be attached.]"

Dated this _____ day of ____________________ <*YEAR*>

Signature

(Company Seal)

In the capacity of

Duly authorized to sign bids for and on behalf of:

5.14. Form 14: Letter for Refund of EMD

Date:
Chief General Manager – ITD
Securities and Exchange Board of India
SEBI Bhavan,
Plot No. C4-A, “G Block”
Bandra Kurla Complex
Bandra (East) - 400 051
India

Ref: RFP for SIT-NET.

We _____________ (Company Name) had participated in the RFP for SIT-NET. Kindly refund and remit the EMD submitted for participation through NEFT/RTGS. The Details of EMD submitted are as follows:

Sl. No.	Bidder Name	Cheque/DD Number	Drawn on (Bank Name)	Amount (Rs)

Bank details to which the money needs to be credited via NEFT/ RTGS are as follows:

Sl. No.		Details
1	Name of the bank with Branch	
2	Account Type	
3	Account Title	
4	Account Number	
5	IFSC Code	

Sign

Name of the signatory:
Designation :
Company Seal :

5.15. Form 15: Consortium details

Sl. No.	**Name of Primary bidder**	**Primary bidder responsibilities**	**Name of Consortium members**	**Consortium member organization details (Office address, contact details, website details)**	**Consortium member organization contact person details (person name, address, email id and contact no.)**	**Tools, Technologies and services provided /managed by consortium member**	**Details of SLA, support level and Service arrangements with consortium member**	**Whether the consortium member is blacklisted firm/company in any Govt. department/Banks/ PSU in India (or in foreign if the member is of foreign entity) (if yes then please provide the details)**
1								

5.16. Form 16: Letter from Consortium Member

(Applicable if consortium is proposed)

To, Date__________

Chief General Manager – ITD
Securities and Exchange Board of India
SEBI Bhavan,
Plot No. C4-A, “G Block”
Bandra Kurla Complex
Bandra (East) - 400 051
India

Dear Sir,

We____________________(Name of consortium member) who are established and reputable manufacturers/service provider of __________________ having head office at ____________ &registered Office in India at ______________do hereby authorize and permit M/s________________________ to submit bid to SEBI in response to their RFP for SIT-NET towards following products/services to be supplied/provided by us as a members of consortium for bidding the RFP.

We also undertake that we have not been blacklisted by the Government Authority or Public Sector Undertaking (PSUs) in India or any Financial Institution in India as on date of submission of response. As a consortium member we will be supplying following products/services:

Sl. No.	Name of Product/Service	Detail

Yours Faithfully

Name of Authorized Representative:

Designation of Authorized Representative:

Signature of Authorized Representative with company seal:
Verified by:

Signature of Verifying Authority:
Date:

5.17. Form 17: OEM Training Details

The OEM Certified training where applicable, should be provided by respective OEMs for at least 4 SEBI IT persons every three year till the tenure of the agreement i.e. two times during the tenure and should also facilitate to undergo formal certification program conducted by respective OEMs without adding any additional cost to SEBI.

Sl. No.	**Proposed product**	**OEM name**	**OEM certification training details [Like Training topic, number of days, modules, etc.]**	**Certification cost included in the training (Yes/No)**	**Nature of Training (Classroom/ web module etc.)**	**Training material provided (Yes/No)**	**Remarks**

5.18. Form 18: Bank Guarantee

To,
Chief General Manager – ITD
Securities and Exchange Board of India
SEBI Bhavan,
Plot No. C4-A, "G Block"
Bandra Kurla Complex
Bandra (East) - 400 051
India

Whereas <Name of the Bidder> (hereinafter called 'the Bidder') has submitted the bid for Submission of RFP -SEBI Enterprise-wide Integrated IT Network Infrastructure SEBI /ITD/HO/2020/12/02 dated December 24, 2020 for SIT-NET at SEBI (hereinafter called "the Bid") to Securities and Exchange Board of India.

Know all Men by these presents that we <Bank Name> having our office at <Address> (hereinafter called "the Bank") are bound unto Securities and Exchange Board of India (hereinafter called "SEBI") in the sum of Rs. <Amount in figures> (Rupees <Amount in words> only) for which payment well and truly to be made to SEBI, the Bank binds itself, its successors and assigns by these presents.

Sealed with the Common Seal of the said Bank this <Date>

The conditions of this obligation are:

1. If the Bidder having its bid withdrawn during the period of bid validity specified by the Bidder on the Bid Form; or
2. If the Bidder, having been notified of the acceptance of its bid by SEBI during the period of validity of bid
    - (a) Withdraws his participation from the bid during the period of validity of bid document; or
    - (b) Fails or refuses to participate in the subsequent Tender process after having been shortlisted;

We undertake to pay SEBI up to the above amount upon receipt of its first written demand, without SEBI having to substantiate its demand, provided that in its demand SEBI will note that the amount claimed by it is due to it owing to the occurrence of one or both of the two conditions, specifying the occurred condition or conditions.

This guarantee will remain in force up to <insert date> and including <extra time over and above mandated in the RFP> from the last date of submission and any demand in respect thereof should reach the Bank not later than the above date.

NOTHWITHSTANDING ANYTHING CONTAINED HEREIN:

I. Our liability under this Bank Guarantee shall not exceed Rs. <Amount in figures> (Rupees <Amount in words> only)
II. This Bank Guarantee shall be valid up to *<insert date>*
III. It is condition of our liability for payment of the guaranteed amount or any part thereof arising under this Bank Guarantee that we receive a valid written claim or demand for payment under this Bank Guarantee on or before *<insert date>*) failing which our liability under the guarantee will automatically cease.

(Authorized Signatory of the Bank)
Seal:
Date:

5.19. Form 19: Masked Bill of Material

The copy of the commercial bid form containing all the products and services to be proposed as part of project with masked price (without mentioning any price details) should be submitted along with the technical bid for the purpose of technical evaluation. If it contains any price information, then the technical bid will be rejected.

6. Appendix II: Financial Bid Templates

The Bidders are expected to respond to the RFP using the forms given in this section and all documents supporting financial bid.

Forms to be used in Financial Proposal

Form 1: Covering Letter
Form 2: Detailed technical BOM with list of products, solutions, services and licenses

The Bidder should furnish the information / quotation as per following format:

1. MANDATORY ITEMS as per item mentioned in section 6.2 Form 2. (for SIT-NET proposed as part of overall solution).
2. Bidders should include all the items required for successful implementation /operationalization of solution as per the scope mentioned in this RFP.
3. If some items are not mentioned in this commercial bid form which are required for successful implementation/operationalization of solution as per the scope of this RFP , then the same should be included as a separate line item in this commercial bid form.
4. If some items are not quoted by the bidders in this commercial bid form which are required for successful implementation/operationalization of overall solution as per the scope of this RFP, then the bidder should provide and maintain (during contract period) such items free of cost to SEBI.
5. The copy of the commercial bid form containing all the products and services to be proposed as part of project with masked price (without mentioning any price details) should be submitted along with the technical bid for the purpose of technical evaluation. If it contains any price information, then the technical bid will be rejected.
6. The bidders are advised not to indicate any separate discount in the commercial bid. Discount, if any, should be merged with the quoted prices. Discount of any type, indicated separately, will not be taken into account for evaluation purpose.

6.1. Form 1: Covering Letter

To:

<Location, Date>

Chief General Manager – ITD
Securities and Exchange Board of India
SEBI Bhavan,
Plot No. C4-A, "G Block"
Bandra Kurla Complex
Bandra (East) - 400 051
India

Subject: Submission of the Financial bid for SIT-NET

Dear Sir/Madam,

We, the undersigned, offer to provide the Implementation services for SIT-NET in accordance with your Request for Proposal SEBI /ITD/HO/2020/12/02 dated December 24, 2020 and our Proposal (Technical and Financial Proposals). Our attached Financial Proposal is for the sum of <*Amount in words and figures*>. This amount is excluding all the applicable taxes.

1. **PRICE AND VALIDITY**
   All the prices mentioned in our Tender are in accordance with the terms as specified in the RFP documents. All the prices and other terms and conditions of this Bid are valid for a period of *120 days* from the date of opening of the Bid.

2. **UNIT RATES**
   Bidders are required to mention unit prices for all the items made under this proposal. Unit price will remain fixed during the entire duration of the agreement and SEBI reserves the right to procure the additional items at same unit price.

3. **BID PRICING**
   We further confirm that the prices stated in our bid are in accordance with your Instruction to Bidders included in Bid documents.

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

5. **BID PRICE**

We declare that our Bid Price is for the entire scope of the work as specified in the Section 2. These prices are indicated Commercial Bid attached with our Bid as part of the Bid.

6. **PERFORMANCE BANK GUARANTEE**

We hereby declare that in case the contract is awarded to us, we shall submit the Performance Bank Guarantee as specified in the Appendix VIII of this RFP document.

Our Financial Proposal shall be binding upon us subject to the modifications resulting from Contract negotiations, up to expiration of the validity period of the Proposal, i.e., May 28, 2021.

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

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

Thanking you.
Yours sincerely,

Authorized Signature:
Name and Title of Signatory:
Name of Firm:
Address:

6.2. Form 2: Detailed Technical BOM with List of Products, Solutions, Services and Licenses

Bidders must fill the price quoted at the appropriate column when it is due for payment.

Table 17: Detailed Bill of Material for the proposed solution

Sl. No.	Item	Make & Version	Quantity	Unit Price (Rs.)	Total Price for 3 years (Installation, Implementation and Warranty & Support Period) in (Rs.)	Applicable Taxes (GST)	4th Year AMC cost (Rs.)	5th Year AMC cost (Rs.)	Nth Year AMC cost (Rs.)	Total price for N yrs AMC (F+G+H …)	Applicable Taxes (GST)	Total Price (E+J) in (Rs.)	Applicable Taxes (GST)	Net Present Value (NPV)
A	**List of Solutions/Technologies**													
1	**Network Devices**													
a	**Infrastructure Devices**													
1.	Server Farm Switch (L3) at SEBI Bhavan 1 (in HA)		2											
2.	Server Farm Switch (L3) at SEBI Bhavan 2 (in HA)		2											
3.	Server Farm Switch (L3) at SEBI DR		1											
4.	Core Switch (L3) at SEBI Bhavan 1 (in HA)		2											

5.	Core Switch (L3) at SEBI Bhavan 2 (in HA)		2											
6.	Access Switch (L2) (48 Ports) at SEBI Bhavan 1		45											
7.	Access Switch (L2) (48 Ports) at SEBI Bhavan 2		25											
8.	Access Switch (L2) (48 Ports) at DR		5											
9.	Access Switch (L2) (48 Ports) at ROs (NRO, ERO, WRO, Mittal Court Office)		15											
10.	Access Switch (L2) (48 Ports) at Local offices and NCL office		20											
11.	Internet Switch at SEBI Bhavan 1 (in HA)		2											
12.	Internet Switch at SEBI Bhavan 2 (in HA)		2											
13.	Internet Switch at DR		1											
14.	Link Load Balancer at SEBI Bhavan 1 (in HA)		2											
15.	Link Load Balancer at SEBI Bhavan 2 (in HA)		2											
16.	Link Load Balancer at DR		1											
17.	IP KVM Switch at SEBI Bhavan 1 (16 Ports)		1											

18.	IP KVM Switch at SEBI Bhavan 2 (16 Ports)		1											
19.	IP KVM Switch at DR (16 Ports)		1											
20.	IP KVM Switch at ROs (NRO, ERO, WRO, Mittal Court Office) (8 Ports)		4											
21.	SFP modules		10											
22.	SFP+ modules		10											
23.	QSFP modules		10											
b	**Operating System**													
	To be put by bidder (If any)													
c	**Software**													
	To be put by bidder (If any)													
d	**Licenses**													
	To be put by bidder (If any)													
Sub Total of Network Devices														
2	**IP Telephony**													

a	**Infrastructure Devices**													
1.	Video IP Phone for Division Chiefs		300											
2.	Non-Video IP Phone for Officers		850											
3.	Video IP Phone for Senior Management		18											
4.	Non-Video IP Phone for Outsource Staff (Data Entry Operators, Electrician, Pantry, SEBI Control etc.)		500											
5.	Non-Video Conferencing IP Phone for Conference Rooms		10											
6.	Voice Server at SEBI HO (in HA)		2											
7.	Voice Server at DR		1											
8.	Voice Gateway Router (L3) at SEBI HO (in HA)		2											
9.	Voice Gateway Router (L3) at SEBI Bhavan 2		1											
10.	Voice Gateway Router (L3) at SEBI Ros (NRO, ERO, WRO, Mittal Court Office)		4											
11.	Voice Gateway Router (L3) at SEBI LOs and NCL office		18											

12.	Other components (Other server, PRI Cards, SIP related cables etc.)													
b	**Operating System**													
	Operating System in DC													
	Operating System in DR													
c	**Software**													
	Software in DC													
	Software in DR													
d	**Licenses**													
	Licenses for IP Telephones and Soft Clients													
	Voice Gateway Router Licenses													
Sub Total of IP Telephony components														
3	**Wi-Fi**													
a	Infrastructure Devices													
	Wi-Fi Controller at SEBI Bhavan 1		2											
	Wi-Fi Controller at DR		1											
	Wi-Fi Access Point at SEBI Bhavan 1		100											
	Wi-Fi Access Point at SEBI Bhavan 2		100											

	Wi-Fi Access Point at DR		10											
	Wi-Fi Access Point at ROs (NRO, ERO, WRO, Mittal Court Office)		40											
	Wi-Fi Access Point at Local offices and NCL office		54											
	Wi-Fi Sensors at SEBI Bhavan 1		To be put by bidder											
	Wi-Fi Sensors at SEBI Bhavan 2		To be put by bidder											
	Wi-Fi Sensors at DR		To be put by bidder											
	Wi-Fi Sensors at ROs (NRO, ERO, WRO, Mittal Court Office)		To be put by bidder											
	Wi-Fi Sensors at Local offices and NCL office		To be put by bidder											
b	Operating System													
	To be put by bidder (If any)													
c	Software													
	To be put by bidder (If any)													
d	Licenses													
	Licenses for Wi-Fi Controller													

	Licenses for Wi-Fi Access Points													
	Licenses for Wi-Fi Sensors													
Sub Total of Wi-Fi components														
4	**Software Defined Network (SDN)**													
a	Infrastructure Devices													
	Infrastructure in DC													
	Infrastructure in DR													
	Infrastructure at other locations (ROs and LOs)													
b	Operating System													
	Operating System in DC													
	Operating System in DR													
c	Software													
	Software in DC													
	Software in DR													
d	Licenses													
	To be put by bidder (If any)													
Sub Total of SDN components														

5	**Network Access Control (NAC)**													
a	Infrastructure Devices													
	To be put by bidder (If any)													
b	Operating System													
	To be put by bidder (If any)													
c	Software													
	To be put by bidder (If any)													
d	Licenses													
	To be put by bidder (If any)													
Sub Total of NAC components														
6	**AD, DNS, DHCP**													
a	Infrastructure Devices													
	AD/DNS server at SEBI Bhavan 1 (in HA)		2											
	AD/DNS server at SEBI Bhavan 2		1											
	AD/DNS server at DR (in HA)		2											

	AD/DNS server at ROs (NRO, ERO, WRO, Mittal Court Office)		4											
	Software		2											
	DHCP server at SEBI Bhavan 1 (in HA)		2											
	DHCP server at SEBI Bhavan 2 (in HA)		2											
	DHCP server at DR (in HA)		2											
	DHCP server at ROs (NRO, ERO, WRO, Mittal Court Office)		4											
b	Operating System													
	To be put by bidder (If any)													
c	Software													
	To be put by bidder (If any)													
d	Licenses													
	To be put by bidder (If any)													
Sub Total of DHCP components														
7	**Network Security solution (Firewall)**													
a	Infrastructure Devices													

	SEBI Bhavan 1 (10 Gbps) (in HA)		2											
	SEBI Bhavan 1 (10 Gbps) (in HA)		2											
	SEBI Bhavan 2 (10 Gbps) (in HA)		2											
	SEBI Bhavan 2 (10 Gbps) (in HA)		2											
	DR-Chennai (10 Gbps) (in HA)		2											
	DR-Chennai (10 Gbps) (in HA)		2											
	ROs (NRO, ERO, WRO, Mittal Court Office) (3 Gbps)		4											
	Local offices and NCL office (1.5 Gbps)		18											
b	Operating System													
	To be put by bidder (If any)													
c	Software													
	To be put by bidder (If any)													
d	Licenses													
	To be put by bidder (If any)													
Sub Total of Firewall components														

8	**Solution for Virtual Private Network (VPN)/ Work From Home**													
a	Infrastructure Devices													
	Infrastructure in DC													
	Infrastructure in DR													
	Infrastructure at other locations (ROs and LOs)													
b	Operating System													
	Operating System in DC													
	Operating System in DR													
c	Software													
	Software in DC													
	Software in DR													
d	Licenses													
	To be put by bidder (If any)													
Sub Total of VPN components														
9	**Video conferencing solution**													
a	Infrastructure Devices													

	Video conferencing unit for Large Conference rooms (More than 10 seaters) at SEBI Bhavan 1	3												
	Video conferencing unit for Large Conference rooms (More than 10 seaters) at SEBI Bhavan 2	3												
	Video conferencing unit for Large Conference rooms (More than 10 seaters) at Mittal Court office	1												
	Video conferencing unit for Large Conference rooms (More than 10 seaters) at ROs (ERO, WRO and SRO)	3												
	Video conferencing unit for Mid- sized conference rooms (6-10 seaters) at SEBI Bhavan 1 and NCL office	13												
	Video conferencing unit for Mid- sized conference rooms (6-10 seaters) at SEBI Bhavan 2	5												

	Video conferencing unit for Mid- sized conference rooms (6-10 seaters) at Ros (ERO, WRO, SRO, NRO) and Mittal Court office	5												
	Video conferencing unit for Mid- sized conference rooms (6-10 seaters) at LOs (17)	17												
	Movable VC unit along with the required cable extension	2												
	Software based video conferencing solution (OEM 1) for Video conferencing meetings (Division based)	125												
	Software based video conferencing solution (OEM 1) for Video conferencing meetings (Individual basis)	1000												
	Software based video conferencing solution (OEM 2) for Webinar	10												
b	Operating System													
	To be put by bidder (If any)													
c	Software													

	To be put by bidder (If any)													
d	Licenses													
	Software based video conferencing licenses (OEM 1)													
	Software based video conferencing licenses (OEM 2)													
	Licenses for Multi party video conferencing upto maximum participants for the partcular end point device													
	Licenses for integration with other web based solution using video endpoints													
	Licenses for collaboration facilities on the Software based video conferencing licenses (OEM 1)													
Sub Total of Video conferencing components														
10	**Patch Management solution**													

a	Infrastructure Devices													
	Patch Management Server at SEBI HO (in HA)		2											
	Patch Management Server at DR		1											
b	Operating System													
	To be put by bidder (If any)													
c	Software													
	To be put by bidder (If any)													
d	Licenses													
	Licenses of Patch Management Software		2500											
Sub Total of Patch Management Components														
Sub Total of Technologies														
B	**FMS-Support Services**													
	L1		13											
	L2		2											
	L3		1											

	Helpdesk		3											
	Technician		1											
Sub Total FMS-Support Services														
C	**Risk Assessment, Mitigation and Audit**													
1	Complete		15											
2	Only VAPT		1											
Sub Total of Risk Assessment, Mitigation and Audit Complete (C 1)														
D	**Annual Maintenance contract (AMC) for the Infrastructure Component of the proposed solution**													
	Annual Maintenance contract (AMC) for the Infrastructure Component of the proposed solution													

Sub Total of Annual Maintenance contract (AMC) for the Infrastructure Component of the proposed solution														
E	**AMC of Existing Network Solution and Network Devices (Refer to clause 2.2.c)**													
1	**AMC for the current (Existing) Network Project covering the entire implementation period (Refer Appendix XIII)**													
2	**AMC support for the project duration for the network devices (Appendix XIV)**													

Sub Total of AMC of Existing Network Devices (Refer to clause 2.2.c)														
F	**Ancillary Services**													
	Ancillary Services													
Sub Total of Ancillary Services														
G	**Training**													
	(Refer clause 3.2.1 E, Form 17)													
Sub Total of Training components														
H	**Change Management**													
	Man month rate for change request													

Sub Total of Change Management Components														
I	**AMC of Passive Network components**													
	Console cable													
	Fiber cable													
	Patch cord RJ45 (1 Meter)													
	Patch cord RJ45 (3 Meter)													
	Power cable (For Network components)													
	Pen drive													
	Patch Panel													
	I/O Socket													
	Connectors													

	Network Multi port switch													
	Other related components													
J	**Buy Back - Buy back cost will be reduced from grand total**													
1	**Floor price for Buyback is 36,55,000/-**													
Sub Total of Buyback Components														
Grand Total Cost of the Project - Buy Back Cost (J)														

Note 6: Bidders are requested to quote the items mentioned in the Bill of Material (BOM) for Local offices however this is optional for SEBI and SEBI may not procure all/some of these items.

7. Appendix III: Present IT Set up

Present Bill of material is attached here for reference-

Present IT Setup with respect to networking components. May be collected by hand.

8. Appendix IV: Manpower Requirement (Responsibility and Competency of Resources)

The bidders should propose on-site resources to be deployed both in PDC and DR including Regional Offices. It is expected that there should be minimal human intervention on day to day operations.

<Experience and certifications for on-site resources is given below>:

Table 18: Manpower Requirement

Sr. No.	Role	Expected Competency	No. of years of experience	Minimum No. of Resources
1	Project Manager	Graduate (Engineering (BE, BTech /MCA) & having ITL certification.	7+ in implementing projects of similar[7] nature	1
2	Solution Architect	Graduate (Preferably Engineering (BE/B Tech) /MCA) & preferably having OEM certifications.	5+ in implementing projects of similar nature	1
3	Technology Expert	Graduate (Preferably Engineering (BE/B Tech) /MCA) & preferably have OEM certification in the proposed technologies	5+ in implementing projects of similar nature	It is expected that at least 1 (one) technical expert per proposed technology with requisite certification to be proposed
4	Security Expert	Graduate (Preferably Engineering (BE/B Tech) /MCA) & having industry standard security certification	5+	1
5	Team Members during implementation	Graduate (Preferably Engineering (BE/B Tech) /MCA)	3+ in implementing network infrastructure and security solutions	Numbers to be provided by the bidder
6	Level 1	Graduate (Preferably Engineering (BE, BTech) /MCA, BSc. IT, BCS) and preferably have certification on relevant	2+	5 at HO and 1 at each RO

---

[7] Projects implementing at least 5-6 of the proposed technologies including SDN or NAC

		technology OEM Certification (Entry level) in Provided technology It is envisaged that the pool of L1 engineers should be proficient and demonstrable in the proposed technology/equipment in SEBI.		
	Level 2	Graduate (Preferably Engineering (BE/B Tech) /MCA) & preferably have OEM certification (Mid-level) in Provided technology, Experience of managing similar nature project	5+	2
	Level 3	Graduate (Engineering (BE, BTech /MCA) & preferably have OEM certification (Highest level) in Provided technology. Experience of managing similar nature projects, experience in troubleshooting and solutioning is required	8+	1
	Video Conferencing Level 1	Any graduate, Diploma qualified and hands on experience managing the Video conferencing systems	2+	4 at HO and on call basis at RO and LO
	Helpdesk	Any graduate, Diploma qualified and hands on experience managing/working in a call centre	2+	3
	Technician	Any graduate, Diploma qualified and hands on experience managing the technical work related to network and cabling.	2+	1

Work profile for onsite FMS Support:

i. Onsite FMS support engineer should have expertise in network devices & network infrastructure maintenance, implementation and troubleshooting.
ii. Daily monitoring of all network devices & network infrastructure across all SEBI Offices.
iii. Prepare checklist and submit to manager for verification.
iv. Prepare monthly reports (MIS reports) on network devices & network infrastructure usage, issues, etc.
v. Logging call and Coordination with SEBI’s helpdesk teams for resolution (Applicable for all offices of SEBI).

vi. Maintain inventory record of all network devices & network infrastructure deployed at across all offices of SEBI.

vii. Network devices & network infrastructure configuration and management etc.

viii. Prepare SLA report including all SLA parameters and submit to IT Manager on monthly/quarterly basis.

ix. The Bidder should submit attendance record of onsite FMS support engineer on monthly basis.

9. Appendix V: Detailed Existing and Proposed Sizing

Sizing with respect to End Users is as follows:

Table 19 : Detailed Existing and Proposed Sizing

Sl. No.	Type of User	Total Number	Usage concurrency (average)	Usage concurrency (Peak)	Growth per Annum
1	Internal Users including	1000	90%	100%	15%
	Mobile users (internal staff)	1000	80%	100 %	15%
2	Out sourced staff [connecting from internal network (LAN or Wi-Fi)]	500	80%	100%	10%
3	External (internet) Users (Approx.) Having access to SCORES web applications	Active registered investors: **84668**[8] Active organisations registered : **13188**#	50%	70%	15%
4	SEBI web server for website (www.sebi.gov.in)	Web server has been designed for 10 Lakh concurrent sessions	30%	70%	10%
5	Distribution of users in SEBI				
5a	Head-office: 4 Locations	400:400:50:10			
5b	RO's 4 Location	50:50:50:50			

---

[8] #as on August 2019

Sl. No.	**Type of User**	**Total Number**	**Usage concurrency (average)**	**Usage concurrency (Peak)**	**Growth per Annum**
5c	LO’s 17 locations Mostly capital cities	100 pax spread across			

10. Appendix VI: Functional and Technical Specifications

10.1. Compliance to Scope of Work

10.1.1. Compliance to Solution for Network Devices

Sr.No.	Description / Specification	Compliance (Yes/No)
1.	The Network devices should support graphical user interface (GUI) with dashboards for Management.	
2.	The Network devices should be compatible with Simple Network Management Protocol Version 3 (SNMP v3).	
3.	The Network devices should be having Stacking capabilities.	
4.	The Network devices must be having POE (Power on Ethernet) capability.	
5.	The Network devices should generate and provide Real Time Multi-Port Statistics on the graphical user interface (GUI) dashboards.	
6.	The Network devices should have Zero Touch provisioning (Plug and Play) when connected in SIT-NET.	
7.	All suitable measures to be in place to ensure ‘No unauthorized access’ while the traffic is moving over MPLS / WAN etc.	
8.	**Link Load Balancer:** The Link Load Balancer solution is required to be deployed in High Availability architecture in Head Office, in order to have complete redundancy as per SEBI’s Network & Security design requirements.	
9.	**Network Racks:** All the Racks have to be supplied for Data Centre deployment only. For floor hub rooms, SEBI’s existing racks would be utilized. SEBI expects that the proposed solution architecture should be optimized in terms of cooling, power, and space (number of racks) requirements. In terms of space it is expected that solution will be implemented in no more than 5 racks.	

10.1.2. Compliance to Solution for IP telephony

Sr.No.	Description / Specification	Compliance (Yes/No)
1.	The solution should provide the below mentioned IP phones along with relevant licenses for hardware as well as soft client (licenses) facility on all the IP Phones: i. Video IP Phone for Division Chiefs ii. Video IP Phone for Senior Management iii. Non-Video IP Phone for Officers iv. Non-Video IP Phone for Outsource Staff (Data Entry Operators, Electrician, Pantry, SEBI Control etc.) v. Non-Video Conferencing IP Phone for Conference Rooms	
2.	The IP Telephony solution should be capable of supporting open standard protocols and support traditional telephony interface such as Analog and IP/Digital, PRI extensions, Trunk interface etc.	
3.	The solution must be deployed in a virtualized platform.	
4.	The solution must provide soft-client facility for Video, Audio calling, Instant Messaging and Presence within SEBI network and outside SEBI network as well from Day 1.	
5.	The solution must connect IP Telephones connectivity across all SEBI offices (HO locations, ROs, Los).	
6.	The solution must integrate with a dedicated Voice gateway for PRI/PSTN calling over MGCP or SIP protocol at each location.	
7.	The solution should have local survivability. The solution must support local Gateway based redundancy for IP Phones and soft phones in case of non-reachability to the central infrastructure.	
8.	Entire solution must support IPv4 & IPv6 from Day 1.	

10.1.3. Compliance to Solution for Wi-Fi Solution

Sr.No.	Description / Specification	Compliance (Yes/No)
1.	Centralized Authentication through AD.	
2.	Wireless access has to be provided based on user role, user groups, based on multiple parameters of AD so that any kind of customized group policy can be pushed	
3.	Rule based controls should be from SEBI's systems and not bidder's cloud based (unless SEBI's IS policy provides for this)	
4.	Configurable capability for defining SSID to specific Access Points	
5.	Automatically shift to adjacent access points if the load is high on particular access points	
6.	Packets are encrypted end to end.	
7.	Wireless intrusion detection/prevention systems can identify and block i. Ad-Hoc Network ii. Dis-association of AP/Client to other network access points. iii. Rogue access points detection & prevention iv. Multiple failure attempts to connect to the wireless network/man in the middle attack. v. Honey Pot attacks. vi. DOS attacks etc	
8.	Bandwidth restriction per user/on group	
9.	QoS throughput traffic prioritization	
10.	Solution shall have MFA based Authentication	

10.1.4. Compliance to Solution for Software Defined Network

Sr.No.	Description / Specification	Compliance (Yes/No)
1.	Software defined solution for centralized configuration, management and monitoring. The solution should support software defined automation and network device life-cycle management. Solution should be capable of plug and play configuration and template based network provisioning. Solution should support advanced wireless troubleshooting using wireless sensors.	
2.	The solution should have Zero Touch provisioning (Plug and Play) when connected in SIT-NET. Solution should have Automated network devices on-boarding. The system should allow for plug and play installation of network devices without requiring any manual configuration.	
3.	Identifying and monitoring Network Topology within site location.	
4.	Encryption of network traffic getting generated within SIT-NET. MACsec based Encryption of network traffic between switch to switch and IP sec based encryption between Firewall to Firewall within SIT-NET.	
5.	The solution should provide functionality to select preferred version of software image and highlight devices deviating from preferred version. System should support GUI based upgrade of switches deployed in SIT-NET.	
6.	Troubleshooting the network slowness/access issues using analysis of network traffic.	

10.1.5. Compliance to Network Access Control (NAC)

Sr.No.	Description / Specification	Compliance (Yes/No)
1.	Onsite Installation and implementation of the solution at DC and DR.	
2.	Dedicated policy management to define and administer security configuration requirements, and specify the access control actions for compliant and noncompliant endpoints. In order to have better control and visibility of unauthorized systems connecting to SEBI network, all the network switch ports, especially those which are connecting to endpoints (user PCs) should be blocked and alerted while any unauthorized devices trying to connect to SEBI network	
3.	Ability to conduct a security state baseline for any endpoint attempting to connect and determine the suitable level of access	
4.	Access control so we can block, quarantine or grant varying degrees of access.	
5.	The Solution should **detect and block** the unpatched, unauthorized systems or devices without proper security softwares (such as antivirus, etc.) when connected to SEBI's network. Example of unauthorized systems are: visitors/outsiders/employee owned personal computers/laptops/mobile phones/iPads/other networking/ Wi-Fi/ Bluetooth devices/ other handheld devices, etc. and servers/devices/networking equipment's of other third party organizations / contractors /service providers /individual trying to connect to SEBI's network.	
6.	The solution should automate the process of on-boarding devices automatically with minimum manual interventions.	
7.	Integration with other security applications and components like SIEM, Anti- APT, Antivirus, AD etc.	
8.	Solution shall use agent-based and/or agentless approach for detection of unauthorized access to the network.	
9.	Solution shall provide forensic evidence on any unauthorized access activity within the network.	
10.	The proposed solution should support local survivability.	
11.	NAC should support all SEBI inventory.	

10.1.6. Compliance to solution for AD, DNS, DHCP

Sr.No.	Description / Specification	Compliance (Yes/No)
1.	Updating of AD files – to be updated and synced with SEBI's SAP feed file on a daily basis.	
2.	Setting up of Active Directory /DNS server at HO and DR in high availability mode and single instance at ERO, WRO and NRO.	
3.	Setting up of DHCP and Certificate server at HO (SEBI Bhavan 1 and SEBI Bhavan 2) and DR in High availability mode, and single instances at Regional offices (Delhi, Kolkata, Ahmadabad and Mittal court)	
4.	The implementation of AD/DNS/DHCP services should be compatible and interoperable within SIT-NET.	
5.	The solution should have local survivability.	
6.	Self Service portal for users password reset and other functionalities to users using MFA.	
7.	System must support monitoring using SNMP v3.	
8.	System must integrate with multiple pass-through authentication options including RADIUS, LDAP, Active Directory, SEBI's SAP HR system (Feed file) etc.	
9.	The implementation should also include setting up Group policies, integration and all the necessary components, etc.	
10.	Proposed solution should be vendor agnostic for integration with network devices (Switch/Router etc.) (solution should not have any dependency on any Network switches/router OEM to operate smoothly).	

10.1.7. Compliance to Solution for Network Security [Firewalls]

Sr.No.	Description / Specification	Compliance (Yes/No)
1.	Security Devices (Firewalls and related equipment) of appropriate configuration should be implemented across all SEBI offices.	
2.	Management of Network security infrastructure and services using web based interface, threat detection and incident response and implementation of the solution at DC and DR.	
3.	Threat Prevention using sandboxing, anti-phishing, anti-virus, anti-bot, analytics and threat intelligence. Focus on blocking malware and application-layer attacks, along with an integrated Intrusion Prevention System (IPS).	
4.	Solution should have built in capabilities to react quickly and seamlessly to detect and react to outside attacks across the SIT-NET and add exceptions for detections.	
5.	Set policies to defend SIT-NET and carry out quick assessments to detect invasive or suspicious activity, like malware, and shut it down.	
6.	Protect in-scope systems from the Internet and from other parts of the SIT-NET’s environment. Configure these systems with security policies that deny all traffic except that required for production applications, and can also apply threat prevention controls required to be in compliance.	
7.	Application Inspection and control, Identity based Inspection and control	
8.	Solution shall provide forensic evidence on any unauthorized access activity within the network as follow: Event timestamp, network events in sequence, packet capture of suspicious communication, malware behaviours, malware type, severity, source and destination of attack.	
9.	The proposed solution should support to monitor traffic from multiple segments like WAN, DMZ, Server Farm, Wi-Fi network, MPLS links etc. simultaneously on a single appliance.	
10.	Location wise Firewall solution distribution is mentioned in section 2.3.7.x	

10.1.8. Compliance to Solution for Virtual Private Network (VPN)

Sr.No.	Description / Specification	Compliance (Yes/No)
1.	VPN solution should have atleast following 3 use cases- i. Access to development environment for developers; ii. Adhoc data collection or upload through API or SFTP, etc. **iii.** Work from Home	
2.	Onsite Installation and implementation of the solution at DC and DR.	
3.	Provide SEBI users (Permanent and Outsourced) with secure remote access (RA) to take advantage of VPN infrastructure service.	
4.	Should have provision for various features facilitating Work from Home facility	
5.	The solution must support a wide variety of endpoint devices and operating systems (Example: Windows, MacOS, Linux etc.).	
6.	The solution must provide seamless access to the internal network and public data resources from managed and BYOD devices.	
7.	The solution must ensure to Authenticate and Policy control that integrates with the authentication resources in use by the organization.	
8.	The solution must provide Cryptographic security to prevent the exposure of sensitive data to unauthorized parties who accidentally or intentionally intercept the data.	
9.	The solution must provide the mentioned features such as User authentication, self-service facility like password reset, differentiated access, Strong encryption for data privacy, hashing for data integrity, Split-tunnelling, Device resiliency, Internet link resiliency, Web Deployment, Advanced Malware and DNS protection, VPN Load Balancing etc.	
10.	Solution should be scalable (Refer to section 2.2.2 Capacity and Sizing).	
11.	Self-service portal and multi factor authentication. OTP should always be generated as 3rd factor authentication.	
12.	Provide split tunnelling features.	

10.1.9. Compliance to Solution for Video Conferencing

Sr.No.	Description / Specification	Compliance (Yes/No)
1.	The solution should be able to deploy hybrid Video architecture where by the confidential meeting will happen on the 'On-premise infrastructure' while the Virtual meetings, Webinars and other meetings will be conducted on any cloud platform like WebEx, MS Teams etc.	
2.	The High Definition Video Conferencing (HDVC) Infrastructure to schedule, conduct and manage Video Conferences centrally, (Mobile and Desktop based) over SEBI Network in a secure way. Solution should allow any HDVC end point to Join any cloud-based providers like WebEx, MS Team, Zoom, Google Meet over SIP/H.323 standard based protocol etc.	
3.	The video conferencing facility should be extended to Webinar and Webcast.	
4.	The HDVC end point should be able to provide plug and play facility so that a Computer (Laptop/Desktop/Other similar devices like Digital Tablets) can be connected to the web based video conferencing applications and use the camera and audio-video features similar to the HDVC end points. The solution must provide Video conferencing end-points devices/units for different capacity rooms like Mid- sized conference rooms (6-10 seaters) and Large Conference rooms (More than 10 seaters).	
5.	For Large Rooms, the dedicated codec based video conferencing end points have to be provided.	
6.	For Mid-sized conference rooms, Plug and Play (USB type high definition video camera and Audio units) video conferencing devices have to be provided.	
7.	Movable VC units along with the required cable extension and trolley.	
8.	The solution with two (2 different OEMs) cloud based/software-based video conferencing facilities must be deployed with organization wide licenses for meeting/webinar/event/webcast.	
9.	The solution should preferably integrate with the IP Telephony platform with centralized phonebook, centralized dial plan, and point to point & multi point calling between IP Phones, HDVC endpoints & soft clients.	
10.	Dedicated On Site FMS support should be provided at Head office and on-call basis to Regional offices and Local offices when required.	
11.	Entire solution must support IPv4 & IPv6 from Day 1.	

10.1.10. Compliance to Solution for Patch Management

Sr.No.	Description / Specification	Compliance (Yes/No)
1.	Integration with SEBI’s Active Directory	
2.	Integration with various systems and solutions implemented across SEBI to fetch the inventory of the endpoints within SIT-NET	
3.	Asset and Inventory Management	
4.	License Metering	
5.	Software Distribution	

10.2. Detailed Functional & Technical Specifications

10.2.1. NAC Solution Functional Specifications:

Sr.No.	Description / Specification	Score	Compliance (Yes/No)	Mandatory (M) or Non-mandatory
Functional Specifications				
1.	Network Access Control (NAC) should have N+1 architecture availability at DC and DR with proposed solution should have purpose build appliances.	2		M
2.	Network Access Control (NAC) should have functionality to self-service device on-boarding from SEBI's employees, guests, outsourcing engineers, etc. The employees should have facilities to get their devices onto the network without requiring assistance from IT support team.	2		M
3.	Network Access Control (NAC) should provide simplified Visitor workflow processes to enable employees, receptionists, guests, and other outsourcing employees to create temporary/permanent accounts for secure wireless and wired network access.	2		M
4.	Network Access Control (NAC) should provide access to device configuration on a need-to-know and need-to-act basis while keeping audit trails for every change in the SIT-NET.	1		
5.	Network Access Control (NAC) should provide Posture Assessment facility to the endpoints connected to the SIT-NET including LAN, WAN, VLAN, and VPN etc. Posture Assessment includes but not limited to the ability to create powerful policies that include, but are not limited to, checks for the latest OS patch, antivirus and antispyware packages with current definition file variables (version, date, etc.), antimalware packages, registry settings (key, value, etc.), patch management, disk encryption, rooted or jailbroken status, application presence, and USB-attached media.	2		M
6.	Network Access Control (NAC) should provide comprehensive authentication and authorization using integration with single sign-on solution or SEBI's active directory solution including but not limited to multiple groups, disjointed domains into logical groups.	2		M
7.	Network Access Control (NAC) should provide a built-in help web console for monitoring, reporting, and troubleshooting having robust historical and real-time reporting for all services. Network Access Control (NAC) should log all the activity	2		M

	and provide real-time dashboard metrics of all users and endpoints connecting to SIT-NET.			
8.	Network Access Control (NAC) should provide agentless web authentication for users which are not getting authenticated through SEBI's active directory solution.	2		M
9.	Network Access Control (NAC) should provide Device Quarantine facility to place noncompliant endpoints into quarantine, preventing the spread of infection while giving the endpoints access to remediation resources.	2		M
10.	Network Access Control (NAC) should provide Centralized Management allowing to define a policy for the SIT-NET as well as the related remediation packages necessary for recovery.	1		
11.	Network Access Control (NAC) should have Remediation and Repair facility on endpoints through periodic evaluation and remediation to provide operating system patches and updates, virus definition files, or endpoint security solutions to compromised or vulnerable devices. Either automated remediation through the optional agent, or instruction based self-remediation by the users.	2		M
12.	Network Access Control (NAC) should provide Device Health Check over wireless, wired and VPN connection and ensure endpoints meet security and compliance policies before they connect to the SIT-NET.	2		M
13.	Network Access Control (NAC) solution should provide Risk scoring of endpoints by analyzing inputs received from VA (Vulnerability Assessment) tool.	1		
14.	Network Access Control (NAC) solution should control access to the network with policies, including pre- admission endpoint security policy checks and post- admission controls over users and endpoint devices.	1		
15.	The following is a list of functions that should encompass a NAC solution:	2		M
	I. Endpoint Detection and profiling - Detecting and profiling new endpoints as they are introduced to the network.			
	II. Authentication – authenticating each user accessing the network no matter where they are authenticating from and/or which device they are using.			
	III. Endpoint Security Assessment – assessing whether a newly introduced network endpoint complies with the security policy of the organization. These checks may include the ability to gather knowledge regarding an endpoint's			

	operating system, the list of installed patches, the presence of anti-virus software and its virus signature date, etc.			
	IV. Remediation– quarantining an element that does not comply with the defined security policy until the issues causing it to be non-compliant are fixed. When quarantined, the endpoint may be able to access a defined set of remediation servers allowing the user fixing the non-compliant issues and to be reintroduced, now successfully, to the network.			
	V. Enforcement – restricting the access of an endpoint to the network if the endpoint does not comply with the defined security policy.			
	VI. Authorization – verifying access by users to network resources according to an authorization scheme defined in an existing authorization system, such as Active Directory, RADIUS servers, etc., allowing the enforcement of identity-based policies after an element is allowed on the network.			
	VII. Post-Admission Protection – continuously monitoring users, elements and their sessions for suspicious activity (i.e. worms, viruses, malware, etc.) by integrating with proxy/firewall/endpoint solution etc.). If detected, the action taken by a NAC solution may vary from isolating the offending system to dropping the session.			
16.	The Network Access Control (NAC) solution should be an automated security control platform that can monitor and control everything on the network—all devices, all operating systems, all users. The solution shall let employees and guests remain productive on the network while critical network resources.	1		
17.	Solution should Maintain an up-to-date/centralized inventory of authorized devices connected to SIT-NET (within/outside SEBI’s premises) and authorized devices enabling the SEBI’s network.	1		
18.	The proposed solution (appliances) will be deployed for SEBI centrally at two locations i.e. Mumbai & Chennai.	1		
Management				
19.	The proposed solution should have a Centralized Management Console with customizable dashboard and role-based admin	1		
Reporting				
20.	The proposed solution must support agent-based and/or agentless deployment and provide complete posture analysis. The Solution Should support the all the feature & Functionalities like Profiling,	2		M

	Compliance check, Alert, Remediation & Blocking etc.			
21.	Solution must be vendor & OS agnostic to existing wired, wireless and VPN network.	1		
22.	Solution must have capabilities to block the endpoint which are connected on Unmanaged Network Infrastructure (Like Unmanaged Switches).	1		
23.	Auto-Remediation or Should guide users through a self-remediation process.	1		
24.	The solution should discover any new device entering the network and permit network access based upon the policy for the device.	2		M
25.	The solution should have the capability to collect endpoint attribute data via passive network telemetry, querying the actual endpoints, or alternatively from the infrastructure	1		
26.	The solution should verify endpoint posture assessment for endpoint devices like PCs/laptops/thin-clients/Printers, Wireless device (router, etc.), Scanner, IP Phone, IP Camera, Tablet, Smart Phone, IOT's (Internet of Things) etc. Connecting to the SIT-NET. The solution should provide the ability to create powerful policies that include but are not limited to checks for the latest OS patches, antivirus and antispyware software packages with current definition file variables (version, date, etc.), registries (key, value, etc.), and applications.	1		
27.	The Solution should be able to discover endpoints on the network, profile them dynamically based in the configured endpoint profiling policies and assign to the matching endpoints identity groups depending on their profile.	1		
28.	The solution must allow user access to the network in a worst case scenario in case of non-availability of AD server/NAC server or any other reasons.	1		
29.	The proposed solution should support the mechanism to send customized message to specified recipient/end users when a certain policy is triggered. For e.g. If NAC policy violation exceed certain threshold limit for certain users, then the user should receive a dialog box message.	1		
30.	The proposed solution should detect known or unknown/rogue devices on specific VLAN depending on device type, MAC address, or other criteria	1		
31.	The proposed solution should be able to Detect infected or otherwise compromised/malicious devices on specific VLAN depending on threat	1		

	information from desktop anti-virus, vulnerability assessment tool, SIEM alerts or other criteria.			
32.	The Solution should have Policy creation tools:	2		M
	1. Policy simulation engine for testing policy integrity			
	2. Wizard based interface			
	3. Pre-configured templates			
	4. Quick look-up of AD attributes			
33.	The Solution shall have capability, which allows NAC admin to add a device on a portal, where the device goes through a registration process for network access. It should also allow NAC admin to mark as lost any device that they have registered in the network, and blacklist the device on the network, which prevents others from unauthorized network access when using the blacklisted device. The Solution should also support removing/adding any device in the enterprise network temporarily, then register the device for network access again later.	1		
34.	The solution should support all versions of Windows Starting for all latest versions of OS windows, Mac OS, Linux etc. versions for complete posture assessment both agent based and/or agent-less.	1		
Integration Capability				
35.	Solution should integrate seamlessly with SIT-NET infrastructure comprising of routers, switches, firewalls, IPS, various types of WAN links and computers, devices, Operating Systems etc. The proposed NAC solution should integrate with leading Firewall brands such as (Checkpoint, Juniper, Palo Alto Networks, Fortinet, Cisco, Citrix, etc.) to respond rapidly to compromised devices on network to prevent threat propagation.	2		M
36.	The proposed solution should support patch/firmware upgraded/plug-in module to add new security features.	1		
Licensing				
37.	Licensing should be based on number of end points /IPs and scalable as per SEBI's requirement. The proposed Solution should be licensed wherein all supported features should be available for all IP devices. Licensing (including any third party product for software, hardware, appliance and database) should cover all the features required to deploy the NAC solution.	1		
38.	The proposed solution should support Help desk and self-service remediation allowing for load reduction for central administrators through end user self-support and automatic remediation.	1		

39.	Solution should provide below mentioned mechanism for notification of user credentials to Guest Users - 1) Web Page redirect 2) SMS integration 3) Email	1		

10.2.2. NAC Solution Technical Specifications:

Sr.No.	Description / Specification	Score	Compliance (Yes/No)	Remarks
1.	The proposed solution should be integrated with SEBI’s PIM solution	2		**M**
2.	The proposed solution must possess an architecture that should works in offline Mode /SPAN/ Mirror Traffic i.e. out-of-band mode.	1		
3.	The solution should have an architecture such that even if the primary server is down, the endpoints should still get policy updates from DR servers without any changes required at their end	1		
Management				
4.	The solution should offer a built-in monitoring,	2		M
5.	The solution should enable administrators to centrally configure and manage profiler, posture, guest, authentication, and authorization services in a single web-based / GUI console, simplifying administration by providing consistency in managing all these services.	1		
Reporting				
6.	The proposed solution must be able to generate Reports on different parameters. i.e. Compliance , Non- Compliance , corporate , Guest , BYOD (Bring Your Own Device) , Mobile Devices, Network Printers, Wireless Access Point (WAP), Scanner, IP Phone, IP Camera, Tablet, Smart Phone, IOT's etc.	2		M
7.	The proposed solution should have ability to generate reports in different formats, such as HTML, Excel, CSV and PDF	2		M
8.	Reports should automatically be generated on a scheduled basis and should be available in real time on demand. The proposed solution should come with predefined, out-of-the-box reports.	1		
9.	Should support scheduled reports be delivered via e- mail	1		
10.	The solution should provide a Registered Endpoints Report. The report should provide the following details:	1		
	· Logged in Date and Time			

	· Portal User (who registered the device)			
	· MAC Address			
	· Identity Group			
	· Endpoint Policy			
	· Static Assignment			
	· Static Group Assignment			
	· Endpoint Policy ID			
	· NMAP Subnet Scan ID			
	· Device Registration Status			
11.	The proposed solution should operate within a heterogeneous network with switches, routers, etc. from multiple vendors. NAC appliance should support vendor agnostic switch infrastructure. It must support the 802.1x mechanism.	1		
12.	The solution should have a provision to support non- NAC capable hosts (i.e., printers, IP phones, IOT's etc.) based on Mac address or other parameter and it should support exception lists for non-NAC capable hosts.	2		M
13.	The solution should support the backup and recovery of policies/configuration.	2		M
14.	Solution shall provide forensic evidence on any unauthorized access activity within the network. For forensic and faster network troubleshooting, the solution should log each & every session/ all important events that pass through and provide simple graphical and statistical reports. Logs should be exportable to external log server. Logs of Deny / Quarantine end points should be generated and exportable in formats like CSV, etc.	1		
15.	The proposed solution should be able to support IPv6-IPv4 dual stack deployments.	2		M
16.	Solution should take feedback from external systems like Syslog servers, SIEM, IDS/IPS, Firewall etc. and block a user if compromised from joining the network.	1		
17.	Device authentication & network access control- The solution must support the following authentication methods: a) 802.1X Authentication. b) Non 802.1X Device Authentication c) MAC Address based Authentication by type d) MAC Address based Authentication by pre-defined list e) AD – LDAP f) Remote Authentication / RADIUS / TACACS / TACACS+, Diameter etc. g) Profiling / Network Device Visibility	1		

18.	The solution should support importing endpoints from a comma-separated values (CSV) file in which the list of endpoints appears with the MAC address and the endpoint profiling policy details separated by a comma	1		
19.	The solution should support MAC Address Bypass (used for devices which do not support 802.1x) and can further utilize identity of the endpoint to apply the proper rules for access.	1		
20.	The solution should have profiling capabilities integrated into the solution in order to detect headless host. The profiling features leverage the existing infrastructure for device discovery. Should support the use of attributes from the following sources or sensors:	1		
	Profiling using MAC OUIs			
	Profiling using DHCP information			
	Profiling using RADIUS / TACACS / TACACS+ information			
	Profiling using HTTP information			
	Profiling using DNS information			
	Profiling using NetFlow information			
	Profiling using SPAN/Mirrored traffic			
Integration Capability				
21.	The proposed NAC solution should integrate with Enterprise level SIEM solution (QRadar) and Syslog server. The solution should be able to share information using standard protocols (Syslog, CEF) and should allow the SIEM system to send syslog messages to the NAC solution to automatically respond to any endpoint security issues	1		
22.	The proposed solution must able to integrate with existing Antivirus solution such as TrendMicro Officescan for Auto- Remediation.	1		
23.	The proposed solution must able to integrate with Service Manager Tool such as HPSM or any other ticketing tool for ticketing/workflow/case management	1		
24.	The proposed NAC solution should integrate with MDM solution at SEBI to provide real-time visibility of unmanaged/agentless mobile devices. In addition, it should also deliver comprehensive information about the managed mobile devices (covering different OS like Android, IOS, etc.) that are connected to the enterprise network. Automatic detection, enrollment, compliance check and policy based access rules regardless of device type.	1		
25.	Solution should integrate with RADIUS server for client device authentication and TACACS+	1		

	for network device authentication and logging. Overlay component may be added to achieve both functionality.			
26.	The proposed solution should be integrated with Privileged Identity Management (PIM) / Privileged Access Management (PAM) solution (CyberArk, Arcos, etc.) / Identity and Access Management (IDAM) solution (CA, etc.).	2		M

10.2.3. IP Telephony Solution Functional requirements:

Sr.No.	Description / Specification	Score	Compliance (Yes/No)	Remarks
	Functional Specifications			
1.	The solution should support Centralized Call Processing and Administration with Distributed Gateways across SEBI offices. The entire solution must support IPv4 & IPv6 from Day1.	2		M
2.	The proposed solution must have the below mentioned features as given below but not limited to these. It can be expand further based on requirement: i. Call forward all, Call forward while busy, Call forward if no answer ii. call pick-up iii. call log (minimum 100 Number of entries per user) iv. hot line v. call waiting indication vi. calling line identification restriction for internal calls and external call vii. conditional external forwarding (busy or no reply) viii. call waiting ix. Boss Secretaries x. do not disturb xi. hunting group xii. immediate forwarding xiii. individual hold xiv. individual call directory/contacts saving xv. internal/external music on hold xvi. last internal/external number redial xvii. Call hold, Call Drop and retrieve xviii. Call Waiting and Retrieve (with configurable audible alerting) xix. Malicious Call ID and Trace xx. Abbreviated Dial, Speed Dial xxi. Call Join xxii. Call status (state, duration, number) xxiii. Missed call information on IP phone xxiv. Local announcement/Music on Hold xxv. Direct inward dialing and Direct outward dialing	2		M
3.	The proposed solution architecture must support Local Survivability where, if Remote location (Other than SEBI HO i.e. SEBI Regional offices or SEBI Local offices) gets disconnected (by means of	2		M

	MPLS/Internet connectivity failure/any other) from DC and/or DR, local audio and video calls must continue to work with limited features that are locally supported by the gateway or server. Minimum of Following or more features must be supported by local survival feature i. Extension to Extension Call (Audio) ii. Extension to PSTN call iii. Call Transfer iv. Call Conference v. Softphone Support with above call features			
4.	The proposed solution should have the capacity to register at least 2000 users on a single instance from day 1. The solution should be capable of scaling up to 7000 users in future without the need of additional hardware.	2		M
5.	User and IP phone extensions must be managed through a synchronized database and GUI.			
6.	The system to have distributed architecture and the centralized control for all the IP PBX entities in the network.	1		
7.	It should be possible for the IP phone to be connected to the desktop. Phone should have dual Ethernet port which will should allow to connect PC/Laptop directly on the 2nd Ethernet port.	2		M
8.	Extension should be able to forward the incoming calls to another internal extension or off-network number	1		
9.	System should be able to generate a group of extensions where they can answer the calls for one another. If one extension is ringing and user is not available to answer that call, other user should be able to answer that call from his own extension.	1		
10.	Users should be able to set do not disturb status on IP Phone.	1		
11.	System should have inbuilt functionality to allow users the freedom to work anywhere, anytime using the cellular phone and calls to office number will be extended to his cell phone number. User should be able to set conditional call extending without intervention of IT support team.	1		
12.	System should allow SIP users to register more than one SIP device with a single extension.	1		

	Minimum 6 devices should be supported to have a single user without using any additional licenses. For example, SIP user can have single extension in office desk phone, mobile softphone, laptop softphone etc. When there is any incoming call, all the devices should ring simultaneously and should support seamless movement from one device to another.			
13.	Users should be able to lock their IP Phone extensions to prevent others from placing outgoing calls their telephone.	1		
14.	Call should be forwarded to voicemail if user is not available to answer the call.	2		M
15.	It should be possible to forward the voicemail to email account.	1		
16.	Proposed solution should allow user wise enablement/configuration of STD, ISD facility with and without security (PIN based access) based on user designation/department/groups.	2		M
	Soft Console for Reception			
17.	Soft console should be proposed at all locations for receptionist to handle the calls. Console allows to handle multiple calls and hold, transfer, conference external callers with the employees. System should also support call parking capability for receptionist. Console should also show the presence status of SEBI employee’s IP Phone.	2		M
18.	Call Preview window should display incoming calls in the queue. Attendant should be able to choose to answer the call from the queue.	1		
19.	When attendant transfers the call to the users and if user is busy then attendant should park the call in the topic queue and when user gets free then transfer the call to the user.	1		
20.	The solution must allow to set up call flow for after office hours and public holidays such that calls can be routed to the main security or any designated department.	1		
Interactive Voice Response (IVR)				
21.	The solution should have IVR facility to configure a personalized IVR message and prompts, Use pre-recorded IVR messages.	1		

Unified Communication and Collaboration (UCC)				
22.	The solution should be SIP-based unified communications client with real time collaboration capabilities that enable business users to easily manage their day-to-day communications from a single interface. High performance multi-model sessions like VOIP, IM/presence, file sharing, screen sharing, web conferencing and point-to-point. The soft-client must be deployed for all employees.	2		M
23.	The UCC Soft client application should be able to make and receive phone calls, point to point video calls and instant messages, host and attend audio conferences.	1		
24.	The UCC Soft client solution should provide availability status for users to see the availability status of their contacts in their contact list. The common supported status for this application should be available, busy, In a meeting, DND etc.	1		
25.	The UCC Soft client application should be available for Desktops (Windows & Mac), as well as for Mobile phones (Android / iPhone).	2		M
26.	The UCC Soft client application should be downloadable from Google Play store or Apple iTunes without any additional cost for any number of devices.	1		
27.	The solution should provide support for open protocols like XMPP and cross federation XMPP.	1		
28.	User should be allowed to mark frequently dialed numbers as "FAVORITES" and same should be displayed in UC client.	1		
29.	UC Client must be able to register on system securely from over internet without VPN.	1		
30.	UC Client must be able to make SIP calls over the internet to video device or meeting address. IT should support features like white-boarding, screen sharing, file sharing, annotations with or without call.	1		
31.	Standard Telephony features such as Call Transfer (Consultative and Blind), Conference, Call Forward, Call hold, Call Park, Call Pickup should be supported on UCC platform.	1		
User Features				

32.	User should be able to log in from any IP Phone using username and password/PIN and all the privilege should extend to that physical IP phone.	1		
33.	IP PBX should support for mobility features providing Simultaneous ringing on both Desk phone and GSM Mobile phone.	1		
34.	Should have voice mail for all users.	2		M
System Features				
35.	The system should support at least 6 digit numbering scheme.	1		
36.	The System should have GUI support web based management console.	1		
37.	Proposed telephony solution must support logical / tenant partitioning. The bidder needs to ensure that Logical Partitioning is implemented properly in the new solution, so that the toll bypass does not happen and the deployed solution meets the government regulations (DoT, etc.).	1		
38.	If enough bandwidth is not available on the private network, then system should automatically use PSTN to establish an internal call.	1		
Security				
39.	The protection of signaling connections over IP by means of authentication, Integrity and encryption should be carried out.	1		
Management				
40.	The solution should enable administrators to centrally configure and manage the IP Telephony services in a single web-based / GUI console for simplifying administration.	1		
Reporting				
41.	The proposed solution must be able to generate Reports on different parameters. i.e. Location wise Users IP Phone allocation list, IP Phone stock list, Location wise IP Phone connectivity status, Software version report etc.	1		
42.	The proposed solution should have ability to generate reports in different formats, such as HTML, Excel, CSV and PDF. Reports should be generated for a custom time period in real time on demand. The proposed solution should come with predefined, out-of-the-box reports.	2		M
43.	The solution should provide a Registered Endpoints Report. The report should provide the following details: · Logged in Date and Time	1		

	· Portal User (who registered the device) · MAC Address · Identity Group · Etc.			

10.2.4. IP Telephony Solution Technical requirements:

Sr.No.	Description / Specification	Score	Compliance (Yes/No)	Remarks
Call processing and call control functionality				
1.	Should support signaling standards / Protocols – SIP, H.323. The solution should have web collaboration facility.	2		M
2.	Voice CODEC support - G.711, G.722, G.729, Opus, iLBC Video codecs: H.264, H.265	2		M
3.	Should have simultaneously audio conferences with at least 10 party in each conference with password/PIN protection. The limit should be configurable for administrator in case of increase in future requirement.	2		M
Video Telephony Features and Support				
4.	The call control system should support integrated video telephony features to the users so that user with IP Phone and video telephony end point should be able to place video calls with the same user model as audio calls.	1		
Software Upgradation				
5.	Bidders should consider software upgrade licenses during the entire period of contract.	2		M
PSTN Connectivity				
6.	The system should be having minimum PSTN Gateway installed. Each PSTN Gateway at SEBI Bhavan 1, SEBI Bhavan 2 should be loaded with 4 x PRI trunk ports and also provide 2 WAN ports to terminate SIP trunks from service provider. Each PSTN Gateway at other locations should be loaded with 2 x PRI trunk ports and also provide 2 WAN ports to terminate SIP trunks from service provider.	1		M
IP Phone-Non-Video Phone for Officers				
7.	The phone should be SIP based. The phone should be Session Initiation Protocol (SIP) protocol based.	1		
8.	Should have 3” or higher diagonal Display.	2		M
9.	Should have full duplex speaker phone and support G.722 Wideband audio along with G.711, G.729/G.729 AB, Opus, audio compression codecs.	1		

10.	The IP Phones shall support connection of Headset.	1		
11.	The IP Phone shall have LED or LCD Indicator for Call Waiting and Message Waiting. The IP Phone should support at least 5 calls in call waiting in the single extension.	1		
12.	The IP Phone shall support Dynamic Host Configuration Protocol (DHCP) based as well as statically configured IP address assignment.	2		M
13.	The IP Phone must have dedicated buttons for directory, mute, volume increase and decrease, voice mail and functions like transfer, conference and hold.	1		
14.	The IP Phone must support one extension number and one additional line that can be configured for another extension, shared line, Boss-Secretary, Speed dial or intercom.	2		M
15.	The IP Phone should provide the directory services to the user by displaying the missed, received and dialed call details including the caller ID and calling time.	1		
16.	It shall be possible to create Local Phone book with pull information from the directory (**Integration with directory like Active directory Contact details etc**.).	2		M
17.	Should support at least POE Class 1 and external AC power adapter option.	1		
18.	The IP phone should have two 10/100/1000 BASE-T Ethernet ports, one for the LAN connection and the other for connecting to PC/laptop.	2		M
19.	The firmware of IP phones shall be upgradable using HTTPS /FTP / TFTP/SFTP.	1		
20.	The phone should support at least 100 entries for call history i.e. missed, received, placed etc.	1		
21.	The IP Phones shall be SNMP manageable directly or through the Communication Server /PBX server. IP Phones or Communication / PBX server shall be able to send IP phone related SNMP logs to the configured Network Management System (NMS). Bidder shall provide generic as well as vendor / OEM specific SNMP MIBs of the equipment for monitoring /management through standard NMS systems along with the equipment.	1		
22.	All users must have access to web portal for setting preferences on IP Phone and managing their own profile and tasks like voice mail and call settings.	1		
Non-Video Phone for Outsource Staff (Data Entry Operators, Electrician, Pantry, Control etc.)				

23.	Should have 3” or higher diagonal Display.	2		M
24.	A phone with display with two lines.	1		
25.	The IP phone should have two 10/100 BASE-T Ethernet ports, one for the LAN connection and the other for connecting to PC/laptop.	2		M
26.	Phone should simplifies call control on the display using soft keys for everyday functions like transfer, conference, forwarding etc.	2		M
27.	Phone should have message waiting indicator	1		
28.	It should have integrated RJ9 headset port with electronic hook switch.	1		
29.	Phone should be configurable via web interface	1		
30.	System Features: Proposed solution/system, End Points shall support features, but not limited to:	1		
	Call waiting			
	Call log on IP Phone (Missed, Received, Dial)			
	Call Conference			
	Auto Call Forwarding			
	Speed dial feature			
	Authorization Code			
	Direct Outward Dialing			
	Music on Hold (Programmable as per the Requirement),			
	Authorization code based long distance dialing			
	Abbreviated Dial			
	Calling line identification			
	Calling party name identification			
	Station Volume controls (Audio, Ringer),			
	call Transfer			
	Hunt Groups			
	Dial Plan Partitioning			
	Hotline			
	Automatic Route Selection			
	Least Cost Routing			

	Alternate Route Selection			
	Movable Extension Number			
	Parallel ringing			
Video IP Phone for Division Chiefs				
31.	Should have minimum 5" or more with a dial pad. The IP Phone must have dedicated button for directory, mute, volume increase-decrease, voicemail and functions like transfer, conference and hold.	2		M
32.	Device should support voice, video.	2		M
33.	It should have RJ9 or 3.5mm or USB port for headset connectivity	2		M
34.	Should have dual RJ45 Ethernet port.	2		M
35.	Should support both IPV4 and IPV6.	2		M
36.	Should have high definition 720p built in camera and support.	1		
37.	Must have integrated camera with shutter option for privacy.	1		
38.	Phone should support Bluetooth connectivity	2		M
39.	The IP Phone must support one extension number and one additional line that can be configured for another extension, shared line, Boss-Secretary, Speed dial or intercom.	1		
40.	Phone should have adjustable stand to allow user to adjust angle perfectly for working distance and camera angle.	1		
41.	It should support message waiting indicator to indicate the presence of unheard voice messages	1		
42.	Device should act as personal wireless access point (Wi-Fi Hotspot) however it needs power adapter to be connected.	1		
43.	Should be able to participate in the video conference call hosted on VC system.	1		
44.	Should run on open architecture and support customization.	1		
45.	Device should support personalization.	1		
46.	Full-duplex speakerphone with wideband audio, Should support POE.	1		
47.	Should have 2 x 10/100/1000 Ethernet LAN ports for connecting LAN and PC.	1		
48.	**Codec Support:** Video: H.264 High Profile, H.264 AVC/SVC Audio: G.711, G.722, G.729a, G.729ab,	1		

	iLBC/Opus			
49.	The IP Phone and IP Telephony solution should be from the same OEM.	2		M
Video Phone for Senior Management				
50.	Should have large screen 5” or above	2		M
51.	Should run on open architecture to offer personalization.	1		
52.	It should offer capacitive touch display to make it easy to operate.	1		
53.	Must have integrated camera with shutter option for privacy.	2		M
54.	Phone should support Bluetooth connectivity.	1		
55.	Phone should have adjustable stand to allow user to adjust angle perfectly for working distance and camera angle	1		
56.	It should support message waiting indicator to indicate the presence of unheard voice messages	1		
57.	Should allow point to point video calls or multiparty conference using conferencing platform	1		
58.	Same device should allow voice and video.	2		M
59.	Should have 3.5mm or RJ9 port or USB for headset connectivity.	1		
60.	It should offer one touch video calling	1		
61.	Should be able to participate in the video conference call hosted on VC system.	1		
Communication Server and Gateway				
62.	The Architecture of the IP Telephony solution must be completely IP based Server & Gateway type communications system.	1		
63.	Proposed system architecture should be based on Open Standard Protocols such as SIP. The proposed system should support SIP based applications, SIP trunks and / or terminals.	2		M
64.	Apart from DC & DR, all other offices locations should provide local survivability in case VPN/MPLS connection between local/regional location & DC/DR goes down or both DC/DR locations goes down. In that case, branch phones should register on local server and provide all standard telephone features, announcements etc.	2		M
65.	All the requirements in respect of complying to the existing DOT/TRAI regulations need to be supported and implemented by the bidder.	2		M
66.	The communication feature server, IP phones and gateway should support IPV4 & IPV6 from day 1.	2		M

67.	The offered system should have Voice compression and decompression in accordance with G.711, G.722, G.729AB, iLBC, Opus wide band audio H.264 ITU-T recommendations and echo-cancellation in accordance.	2		M
68.	System should support the QOS features for the VOIP implementation. it should be compliant with both QOS standards (layer 2 – 802.1 p/q) and layer 3- diffserv/tos).	1		
69.	System should have encryption security with minimum 128-bit key security for both signaling and voice with in a node for all IP subscribers.	1		
70.	Any end of sale and end of support product should not be proposed.	1		
71.	System should support multi device registration where users should be able to register with same extension number without consuming additional licenses.	1		
72.	System should allow users to register from their soft clients even when they are out of the office and without any need of the VPN.	2		M
73.	Should be compatible with all telecom interfaces or Telecom Service providers and It should be compatible with ISDN PRI, Analogy trunks, H.323 trunk, SIP trunk.	1		
74.	The system shall be able to provide interface to ISDN PRI	1		
75.	The system shall have inbuilt web- based software for administration and maintenance of the system. It shall provide reports about station alarms, trunk analysis, processor occupancy, system capacity etc.	2		M
76.	The system should provide complete inbuilt encryption capabilities or features without any external firewall, with the ability to encrypt all traffic (media and call control signaling) between IP phones, soft phones, call controllers and all other associated endpoints via a strong encryption algorithm like IP Sec or SRTP etc.	1		

10.2.5. Network Security Solution Functional requirements

Sr.No.	Description / Specification	Score	Compliance (Yes/No)	Remarks
Management				
1.	The solution should be able to provide web based UI to monitor, analyze and complete an operation	2		M

	using automation scripts/commands/application/etc.			
2.	i. Threat detection and incident response life-cycle management ii. Scale (devices under management, number of administrators, and number of roles/teams involved in operations) iii. Change management, workflow and segregation of duties iv. Automation and orchestration: With third-party IT and Security solutions, and with data center virtualization, cloud and DevOps automation. v. Compliance and audit control validation and reporting vi. Template based configuration support for common policy deployment	1		
3.	The management architecture should support: i. Combined threat prevention and segmentation policies in a unified policy table across appliances, virtual and cloud ii. Consolidated event management and export event policy wise status details iii. Group-based delegation of administration authority, with full workflow support iv. Orchestration integration for virtual environments, including automated services insertion v. Open APIs for integrations with other technologies and systems	1		
Threat Prevention				
4.	The solution should provide integration of robust threat prevention using the below mentioned threat prevention techniques: i. Sandboxing, ii. Anti-virus iii. Anti-Ransomware iv. Anti-bot v. Threat intelligence and analytics vi. Integrate with third party NAC	2		M
5.	The solution should support below mentioned capabilities that include:	2		M

	i. real-time dynamic security intelligence including our firewalls, security gateways, mobile and endpoints ii. detect malware well beyond AV and static analysis iii. blocks even zero-day attacks before they can begin their evasion techniques			
Application Inspection and Control				
6.	The solution must be able to provide application level support that is broad (as many applications as possible), deep (sub-functions within applications), intelligent (able to find the application even if evasion technology is used) and dynamic (frequent updates as applications proliferate or change).	1		
7.	The solution should be able to alert users in real-time about application access limitations, and query them and take feedback as to whether application use is for business or personal use.	2		M
Identity based Inspection and Control				
8.	The solution must support policies based on users or (more importantly) groups of users-based on authentication and authorization against SEBI's active directory solution including but not limited to multiple groups, disjointed domains into logical groups. Policies such as these are tremendously beneficial as they automate typical processes (user moves/add/changes),and decrease configuration changes required on the firewall.	2		M
Scalable performance with advanced security functions				
9.	The solution must be able to easily scale performance as requirements increase, and that hardware and software limitations should not prevent from deploying the latest threat prevention technologies and algorithms.	1		
Encrypted Traffic Inspection				
10.	The solution must be capable of inspecting traffic both to apply control policy and for threat prevention. It also must be sophisticated enough	1		

	to support complex policies such as selective decryption so that certain traffic (e.g. employee's on-line banking) can be excluded from decryption to avoid regulatory or liability pitfalls.			
11.	The solution must include standard encryption and decryption protocols like: SSL/TLS, HTTP etc.	2		M

10.2.6. Network Security Solution Technical requirements:

Sr.No.	Description / Specification	Score	Compliance (Yes/No)	Remarks
Firewall Specification				
General Specifications				
1.	The NG Firewall solution should support IPV4, IPv6 routing protocols	2		M
2.	The NGFW appliance should have console port with RJ45/USB	1		
3.	Appliance should be rack mountable and necessary mounting kit, support side rails should be supplied along with firewall	2		M
4.	Firewall should support VLAN tagging	2		M
5.	**Firewall of category A** should have 12x10 GE SFP+ and 12x1GE Copper interfaces. 10 Gbps firewall throughput with NGIPS capability and application detection enabled.	2		M
6.	**Firewall of category B** should have 4x1GE SFP and 8x1GE RJ45 interfaces. 3 Gbps firewall throughput with NGIPS capability and application detection enabled.	2		M
7.	**Firewall of category C** should have 2 x 1 GE SFP interfaces and 8x1 GE RJ 45 ports. 1.5 Gbps firewall throughput with NGIPS capability and application detection enabled.	2		M
Firewall Features				
8.	Firewall should support creating access-rules/policies with IPv4 & IPv6 objects, users and groups, Geolocation, URL, Domain name, service ports	1		
9.	Firewall should support operating in routed & transparent mode	1		
10.	Should support Static, OSPF, OSPFv3 and BGP	1		
11.	Firewall should support different types of NAT including, Static NAT, Dynamic NAT, Source Address Translation, Bi-Directional/twice nat, Destination Address Translation, NAT46, NAT64	1		

12.	Firewall should support Multicast protocols like PIM, Sparse mode	1		
13.	Should support capability to limit bandwidth on basis of applications, Networks / Geo, service Ports, user & group etc.	1		
14.	Firewall should support creating access-rules with IPv4 & IPv6 objects and time/scheduled based policy	1		
15.	Firewall should support policy-based routing	1		
16.	Proposed firewall must support SNMP v3	2		M
17.	Proposed firewall must support push the logs to Syslog server	1		
18.	Firewall should support Restful API integration	1		
19.	The Firewall should integrate with Multi-Factor Authentication (MFA) to help prevent attack on SIT-NET.	1		
20.	All category of Firewalls must have ability to handle at least 40000 + IPS signatures out of the box excluding custom signatures to address the current and future vulnerabilities and threat landscape.	1		
21.	All category of firewalls should be able to identify attacks based on Geo-location and define policy to block on the basis of Geo-location	1		
22.	Proposed vendor should have an inhouse threat intelligence team and offer built-in capabilities on firewall to integrate with various security threat feeds using STIX/TAXII	1		
23.	Proposed Firewall should not be proprietary ASIC based in nature & should be open architecture based on multi-core CPU's	1		
24.	Solution should be able to provide a complete trajectory of malware file propagation which helps identify the targeted endpoint IP including the providing details of process and trajectory of spread across endpoints without any agents.	1		
Performance & Scalability				

25.	Firewall must be licensed with all the security suite including IPS, AMP, AVC, URL filtering.	1		
26.	**Concurrent Sessions**			
27.	**Firewall of category A** should support 3 Million concurrent sessions with Application detection enabled. Firewall Should have 50000 new connections per second.	2		M
28.	**Firewall of category B** should support 1 Million concurrent sessions with Application detection enabled. Firewall Should have 25000 new connections per second.	2		M
29.	**Firewall of category C** should support 200K concurrent sessions with Application detection enabled. Firewall Should have 5000 new connections per second.	2		M
30.	Firewall need to handle minimum 5 virtual instances/contexts/Virtual Routing Table	1		
31.	Proposed NGFW solution must be capable to detect device failure, link and path failure	1		
32.	Proposed Firewall shall synchronize the following for HA: a) All sessions b) Decryption Certificates c) All configuration changes d) Forwarding Information Base (FIB) tables	1		
NG Firewall filtering requirements				
33.	Should support the filtering of TCP/IP based applications with standard TCP/UDP ports.	2		M
34.	Filtering capability that includes parameters like source & destination addresses, source & destination port numbers, protocol type.	1		
35.	NG Firewall should be able to filter traffic even if the packets are fragmented.	1		
36.	Should support the VOIP Applications by allowing/blocking the SIP, H.323, MGCP and Skinny flows.	1		
NG Firewall- Network Protocol/Standards Support requirements				
37.	All applications should be supported for filtering like Telnet, FTP, SMTP, http, DNS, ICMP,	1		

	DHCP, ARP, RPC, SNMP, Lotus Notes, Exchange, Outlook etc.			
38.	Local access to the NG Firewall modules should support authentication protocols – LDAP, RADIUS & TACACS+.	1		
Administration, Management and Logging				
39.	Proposed Firewall must provide access to Web-UI/ webui & GUI client to configure full functional firewall.	1		
40.	Proposed firewall must support local web-UI & SSHv2 access to configure / troubleshoot onbox, incase if central management console is not reachable	1		
41.	Support for role-based administration of firewall	1		
42.	Firewall administration software must provide a means of viewing, filtering and managing the log data. Logs must provide visibility into threats and detailed analysis. Logging and reporting must be able to showcase real-time, time-based, visibility based on username, SRC-IP, DST-IP, applications, Threats	1		
43.	firewall logs must contain information about the firewall policy rule that triggered the log.	1		
44.	Firewall must provide a minimum basic statistic about the health of the device and the amount of traffic traversing the NGFW device.	1		
45.	Should provide real time health status of all the firewall modules on the dashboard for CPU & memory utilization.	2		M
46.	Should provide state table, total number of concurrent connections/second and the new connections/second counter.	1		
47.	Firewall must send mail or SNMP traps to Network Management Servers (NMS) in response to system failures or threshold violations of the health attributes.	1		
48.	Firewall should be able to integrate with industry standard firewall analyzer tool	1		

49.	Firewall should be able to integrate with Identity Services Engine	1		
50.	Firewall must integrate with PIM solution	2		M
51.	Logging and reporting must support Indicator of compromised support, to provide visibility of host end-point machines which are infected. And must be updated on logging and reporting solution regularly via internet, without manual intervention.	1		
52.	Configuration changes, backups should be done automatically & regularly.	1		
High Availability/clustering				
53.	Firewall should support active/standby high availability/clustering.	2		M
54.	Firewall should support redundant interfaces to provide interface level redundancy before device failover.	1		
55.	Firewall should replicate Nat translations, TCP, UDP connection states, ARP table and SIP signaling sessions.	1		
56.	Firewall should support failover of IPv4 & IPv6 sessions.	1		
57.	Firewall should be having dual power supply. and should have integrated redundant hot swappable power supply.	2		M
58.	Firewall OS need to be upgraded without downtime and There should be no downtime in the network when the firewalls in HA are getting upgraded from one version to another version	2		M
59.	Cluster failover or firewall failover should be without downtime	1		
Hardware Specifications				
60.	Firewall should have 1 x Gigabit Ethernet copper port Integrated network management ports	1		
61.	Firewall must support sufficient local SSD storage for firewall software and temporary logs.	1		

62.	Firewall Management Solution must support sufficient local SSD storage for 3 months of syslogs, audit logs, traffic logs.			
Support Specifications				
63.	The OEM must provide 24 X 7 X 365 technical support. The OEM must provide Direct Enterprise Premium Support to SEBI with dedicated login credentials with highest level permissions to search knowledge base, downloading of the patches, documents and to manage the device. SEBI should be able to raise tickets directly to OEMs.	2		M

10.2.7. AD/DNS/DHCP/IPAM Functional & Technical requirements:

AD				
Sr.No.	**Description / Specification**	**Score**	**Compliance (Yes/No)**	**Remarks**
1.	Solution must support standards-based AD services.	2		M
2.	Solution must support setting up Group policies, integration and all the necessary components, etc.	2		M
3.	The solution should provide self-service portal for password Management, Notification of password expiration and password change.	2		M
4.	Updating of AD files – to be updated and synced on daily basis. Presently a feed file from SEBI's HR system is generated daily, all AD's to be updated accordingly.	2		M

Internal DNS Server				
Sr.No.	**Description / Specification**	**Score**	**Compliance (Yes/No)**	**Remarks**
1.	Solution must support standards-based DNS services and must support the ability to act as an internal Authoritative name server.	2		M
2.	The Solution must support Master-Slave, Multi Master or Stealth Mode deployment architecture and must be able to automate common tasks such as maintaining synchronization between forward and reverse records.	2		M
3.	Authoritative Name Servers must have the built-in protection using Response Rate limiting.	2		M
4.	The solution must allow adding the following types of zones: Forward Mapping (Authoritative, Forward, Stub), Reverse Mapping (IPv4 and IPv6)	2		M
5.	Authoritative Name Servers must have the built-in protection using DNS DDoS protection - DNS Amplification/DNS reflection/Flooding attacks - UDP, TCP and ICMP/ DNS tunneling/ DNS Reconnaissance	2		M

6.	The Solution must support A, NAPTR, SRV, NS, MX, CNAME records	1		
7.	The Solution must support IPv6: AAAA, PTR, host, ip6.arpa, DDNS records and must support multiple DNS views based on IPv4/Ipv6 Addresses.	1		
8.	The Solution must support Instant propagation of changes to the architecture, such as ACLs, DNS Server Options, Forwarders, etc.	1		
9.	The solution must support easy search, sort and filter on any DNS Zone or RR, using any field. The product must support the ability to control DNS logging: DNS query and response logging	1		
10.	The solution must provide a simplified/streamlined process to identify and manage DKIM, DMARC, ADSP, SPF and/or other similar DNS TXT records.	1		
11.	The system must be able to display all hosted DNS Resource Records in one GUI pane	2		M
12.	The Solution must have Import Wizard be built-in solution by the DNS Appliance and should not require any external Java program or external Virtual Machines	1		
13.	The solution must provide a means to track changes to made via Dynamic DNS record assignment. The solution must have inbuilt reports & Status.	1		
14.	System must support System logs forwarding/redirection of logs to a defined syslog host	1		
15.	The solution must support the standard DNSSEC specifications for serving of DNSSEC signed zones and the pass through of client resolution of external zones.	1		
DHCP				
1.	The solution must provide an easy to use "import wizard" to import DHCP records from legacy DHCP Solution.	1		
2.	Import Wizard solution must be supported by the DHCP Appliance and must not require any external Java program or external Virtual Machines.	1		
3.	The DHCP solution must provide high availability along with geo-failover.	2		M
4.	The DHCP solution must be integrated with SEBI’s PIM solution.	2		M

5.	The solution must track and log all user changes to DHCP configurations. The audit logs must be able to identify the change(s) made, the user/system making the change, and a timestamp. The solution should also be able to identify the client IP address from where the change was made.	1		
6.	The solution must be able to perform Dynamic DNS for both IPv4 and IPv6 while linking all associated IP addresses to a single device/object.	2		M
7.	The solution must graph (visually display) the different scopes based on number of IP's used/available over a set period. The solution must provide device finger printing and display or report the data in the GUI.	1		
8.	The DHCP solution must support one IP per MAC address (one lease per client). The DHCP solution must be able to release the DHCP lease if the MAC address has moved to another IP.	2		M
9.	The solution must provide the ability to detect or block devices attempting to use DHCP based on various attributes. These attributes must include MAC address but can include device fingerprint, DHCP options, etc.	1		M
10.	The DHCP Solution must integrate to IPAM for lease consolidation and capacity planning	2		M
11.	The DHCP Solution must have its built-in security mechanism against Rogue Clients performing DHCP Storm attacks without the need for additional licenses	2		M
12.	The DHCP Solution must be able to send alerts in case of DHCP related attacks, high and low threshold alerts	1		
13.	The solution must support creating DHCP custom options. The DHCP Solution must have inbuilt Reports & stats.	1		
IPAM				
1.	The IPAM Solution must support minimum 2,50,000 IP Address Management for both IPv4 & IPv6 together.	1		
2.	The IPAM solution must provide high availability across DC & DR	2		M
3.	The solution must be flexible to allow the creation of custom fields for objects in IPAM. This must be configurable via the Web GUI. The IPAM solution should be able	2		M

	to seamlessly integrate with DNS and DHCP Records.			
4.	The solution must include an application programming interface (API) in order to interface with network and/or asset management systems, a configuration management database (CMDB) solution or other applications.	1		
5.	The IPAM solution should be able to create its own widget to display customized subnet reports, free IP, used IP.	1		
6.	The IPAM solution should have the ability to locate the available subnets inside a Supernet. This is to provide assistance to SEBI when creating subnets inside an aggregated Network.	1		
7.	DDI IPAM user interface must be web-based without specific browser vendor requirements.	1		
8.	DDI IPAM system should support seamless failover between DC and DR.	1		
9.	DDI IPAM system should support VLSM (Variable Length Subnet Masks).	1		
10.	DDI IPAM system should be able to export reports in PDF, CSV format.	2		M
11.	DDI IPAM system should have support for workflow process for various administrator roles and should include a change approval oversight capability.	2		M
12.	DDI audit records should contain a timestamp, username and record modified. DDI Reporting engine should include audit reports.	2		M
13.	DDI system should support granular rights administration limiting the function and rights to user and record level	1		
14.	IPAM Solution should provide centralized Inventory reporting showing which device is assigned to which IP address within the network at any time.	1		
15.	The tool must have the capability to find free address space across a range	2		M
16.	The IPAM Solution must provide integration with devices (Switch/Router) and provide at least following:	1		
	Should show IP Details			
	IP Address			

	DNS name			
	Last alive time			
	Status (Used, Unused)			
	Location name			
	Should show Device Details			
	Mac Address			
	Device type			
	Device name			
	Port Number			
Network Discovery, Inventory, Backup and Archiving				
17.	Solution should have the ability to add network devices into inventory via auto-discovery. The proposed infrastructure should be able discover n network devices. Solution should have the ability to add network devices into inventory via manual add/edit/delete methods. The IPAM Solution component must perform host discovery using a variety of methods including ping, TCP port 80 connections, Address Resolution Protocol (ARP), cache data, and device OS mapping	2		M
18.	Solution should have the ability to add network devices into inventory via integration with third-party products that perform an auto-discovery	1		
19.	Solution should have the ability to capture, archive and view device properties for devices in inventory (for example, changes to OS version, IP address, hostname, textual configuration files, and hardware, software and modeled) for devices in inventory	1		
20.	Solution should have the ability to create and manage custom/manual attributes per device (e.g., asset ID#, street address, State/Province, region, etc.)	1		
21.	Solution should be able create reports be generated in different formats. (PDF, XLS, CSV and HTML formats)	1		
User and End Tracking and Port Analysis				
22.	Solution should offer infrastructure device port consumption tracking and overview, display port usage history	2		M
23.	Solution should offer end host/MAC address location identification and tracking. Solution should offer end host/MAC address location history and auditing	1		

24.	Solution should enable port availability calculations based on configurable periods consistent free time	1		
25.	Solution should report on new and no-longer-present devices on the network	2		M
26.	Solution should highlight location and status changes of devices and interfaces	1		
27.	Solution should have the ability to search by hardware and software attributes.	1		
28.	Solution should provide following reports at minimum:	1		
	End host history			
	Device inventory/components/port capacity			
	DHCP lease history			
	DHCP usage trend			
	DHCP usage statistics			
	DHCP top utilized range			
	DHCP fingerprint – trend			
	DNS reply trend			
	DNS Cache hit ratio trend			
	DNS Query Rate			
	DNS top Clients			
	DNS Top Clients per domain			
	DNS Statistics/zone			
	IPAM network usage statistics			
	IPAM usage trend			
	IPAM top utilized networks			

10.2.8. VPN Solution Functional & Technical requirements:

Sr.No.	Description/Specification	Score	Compliance (Yes/No)	Remarks
Capacity				
1.	The Solution should have the capability to handle individually 1500 concurrent users and should be in a position to handle minimum 2000 users and unlimited applications each from day-1. The System should be supplied with necessary power cards, cables, bracket accessories and other appropriate accessories.	2		M
2.	The proposed SSL VPN Appliance must include all the hardware, software, services and other components necessary to meet the given requirements and to carry out the necessary activities as described in this section as well as the deliverables section given below. Activities must cover whatever is necessary to build the solution, deliver, train, and support SEBI personnel for the period of the contract.	1		
Security				
3.	The solution Should support encryption ciphers:DES, 3DES, AES, Configurable session length, Hashes: MD5, SHA -2. The solution should support IKEv2 VPN protocols or SSL/IPSec VPN protocols.	2		M
4.	The solution should support integration with Multi Factor authentication.	2		M
5.	The solution should support directories: Microsoft Active Directory, LDAP (Active Directory, IBM, etc.); Dynamic groups based on LDAP/AD queries; DAP access attributes and the group-policy inheritance hierarchy.	2		M
6.	The solution should have access control features: User and group, Source IP and network, Destination network, Service/Port (On Demand and Connect only) Define resources by destination URL, host name or IP address, IP range, subnet and domain, Day, date, time and range, Browser encryption key length, Policy	1		

	Zones (allows, denies and quarantines access), File system access controls.			
7.	The solution should have provisions to set number of devices per user which may be VPN enabled based on groups/user role.	1		
Access and Application Support				
8.	At least one built-in VPN client should be supplied along with VPN Server; The supplied client solution should support all leading Operating Systems available now.	2		M
9.	Should support IPv4 and IPv6.	2		M
10.	User authentication should be available for clients; should support token-based authentication.	1		
11.	Encryption should support for data in transit	2		M
12.	Should support on-board migration of existing data, application and other information from current platform to new platform.	1		
13.	Should support unlimited applications.	2		M
14.	Option for Clientless Connectivity should be there.	1		
15.	Should have feature to support to pre-installed agent provides access to any TCP or UDP based application (Windows, Macintosh and Linux support).	1		
16.	Should provide on-client protection for both protected and direct internet traffic	1		
17.	Should support mobile devices including Android/iOS/Windows.	2		M
Management and Administration				
18.	Should have feature for centralized web-based management for all VPN sessions.	2		M
19.	Should support Advanced Reporting and Dashboards.	2		M
20.	Should provide device resiliency - support failover between the active and standby units of a	1		

	resilient firewall pair in the event of a hardware failure.			
21.	Should have feature for User connection monitoring, event alarms, View logs and performance information via the centralized Management Console.	1		
High Availability				
22.	Should support for high-availability with built-in load-balancing and stateful authentication failover.	2		M
23.	Always-on VPN - if the device is on an untrusted network, the client automatically tries to establish a VPN connection to the primary site. The user needs to provide authentication, but no other intervention is required. If the user disconnects, no other network access is permitted.	1		

10.2.9. Solution for Wi-Fi Functional & Technical Specifications

Sr.No.	Description/Specification	Score	Compliance (Yes/No)	Remarks
	Wi-Fi Controller Specifications			
1.	Must be compliant with IEEE CAPWAP or equivalent for controller-based WLANs.	2		M
2.	Should have atleast 1 x MultiGigabit/ 10 gigabit Ethernet interface along with 4x100/1000 RJ45 BaseT ports.	1		
3.	Controller should support minimum 5000 concurrent devices.	2		M
4.	WLAN controller should have scalability to support 500 Access points from day 1 without any hardware change.	2		M
5.	WLAN controller should provide Application visibility with both traffic forwarding mode i.e. when traffic coming to controller and when traffic moving locally from AP to connected access switch. Admin should have option to create policies to allow or deny access based on applications.	1		
6.	WLC should support AP License Migration from one WLC to another	2		M
7.	WLC should support L2 and L3 roaming for IPv4 and IPv6 clients	1		
8.	Controller should support automatic radio channel adjustments for intelligent channel switching and real-time interference detection.	1		
9.	Controller Should support policy-based forwarding to classify data traffic based on Access Control Lists (ACLs).	2		M
10.	To deliver optimal bandwidth usage, reliable multicast must use single session between AP and Wireless Controller. Must support coverage hole detection and correction that can be adjusted on a per WLAN basis.	1		
11.	Must support 802.11 ax (Wi-Fi 6 and above)	2		M
12.	Must be able to restrict the number of logins (connections) per user.	1		
13.	Should provide visibility to Network airtime in order to set the airtime policy enforcement. Must support dynamic Airtime allocation on per WLAN, per AP, Per AP group basis.	1		
14.	WLC performance should remain the same if encryption is on or off for wireless SSIDs.	1		

15.	WLC Should support Rogue AP detection, classification and standard WIPS signatures.	2		M
16.	Should be able to set a maximum per-user bandwidth limit on a per-SSID basis.	2		M
17.	Must support user load balancing across Access Points.	1		
18.	Must support client roaming across controllers separated by a layer 3 routed boundary.	1		
19.	Must support AP over-the-air packet capture for export to a tool such as Wireshark/equivalent	2		M
20.	Shall support the ability to classify different types of interference within 5 to 30 seconds. Should provide real-time charts/log showing interferers per access point, on a per- radio, per-channel basis.	2		M
21.	Support for configuring media streams with different priority to identify specific video streams for preferential quality-of-service treatment.	1		
22.	Should support MAC authentication to provide simple authentication based on a user's MAC address.	2		M
23.	WLC should be able to exclude clients based on excessive/multiple authentication failure.	1		
24.	Should support AP location-based user access to control the locations where a wireless user can access the network	1		
25.	WLC Shall support WIDS & WIPS, and spectral analysis from day 1.	1		
26.	WLC should detect and protect an Ad-hoc connection when a connected user forming a network with other system without an AP or try enabling bridging between two interfaces	1		
27.	WLC should detect and protect and take appropriate containment action if a smartphone user using tethering to connect another device.	1		
28.	WLC should detect and protect if a user tries to spoof mac address of valid client or AP for unauthorized access/authentication.	1		
29.	Should support SNMPv3, SSHv2 and SSL for secure management.	2		M
30.	Should support encrypted mechanism to securely upload/download software image to and from Wireless controller.	1		
31.	Should provide visibility between a wired and wireless network using IEEE 802.1AB	1		

	Link Layer Discovery Protocol (LLDP) and sFlow/equivalent.			
32.	Should support AP Plug and Play (PnP) deployment with zero-configuration capability. Should support AP grouping to enable administrator to easily apply AP-based or radio-based configurations to all the APs in the same group.	1		
33.	Should support selective firmware upgrade APs, typically to a group of APs minimize the impact of up-gradation	1		
34.	Should have a suitable serial console port/micro USB or RJ45 console port.	1		
35.	Should have Voice and Video Call Admission and Stream prioritization for preferential QOS	2		M
36.	Controller should support deep packet inspection for all user traffic across Layer 4-7 network to analyses information about applications usage, peak network usage times for all access points from day one with different traffic forwarding modes i.e. central switching with WLC and local switching when traffic moves locally from AP to connected switch.	1		
37.	Should support IPv4 & IPv6	1		
38.	Should be able to do application visibility for application running behind HTTP proxy. Should support visibility and control based on the type of applications. Support profiling of wireless devices based on known protocols like HTTP/DHCP to identify clients	1		
	Wi-Fi Access Point Specifications			
39.	Access Points proposed must include radios for 2.4 GHz and 5 GHz. Must support Wi-Fi 6 standard.	2		M
40.	An access point must include a standard OEM provided Mounting brackets for mounting on Ceiling or Roof top.	1		
41.	Access Point shall support Console port that uses Standard Port (RJ-45) type connection and Serial console interface or micro-B USB physical jack) type connection.	2		M
42.	Should have one RJ-45 auto-sensing 10/100/1000 (or more) Mbps LAN port. Access Point should have USB port for future requirement.	1		
43.	Must have at least 3 dBi Antenna gain on each radio.	1		

44.	Must support 4x4 MIMO for both 2.4 GHz and 5 GHz radio with Wi-Fi 6.	2		M
45.	Must support minimum of 22dbm of transmit power in both 2.4Ghz and 5Ghz radios. And should follow the local regulatory Norms.	2		M
46.	Must support AP enforce load-balance between 2.4Ghz and 5Ghz band. Must have -97 dB or better Receiver Sensitivity.	1		
47.	Should support locally significant certificates on the APs using a Public Key Infrastructure (PKI).	2		M
48.	Access Points must support Hardware/Software-based encrypted user data and management traffic between controller and Access point for better security. Same model AP that serves clients must be able to be dedicated to monitoring the RF environment.	1		
49.	Must be plenum-rated (UL2043).	1		
50.	Must support 16 WLANs per AP for SSID deployment flexibility.	1		
51.	Access Point Must continue serving clients when link to controller is down.	1		
52.	Must support telnet and/or SSH login to APs directly for troubleshooting flexibility.	2		M
53.	Should support 802.11e and Wi-Fi Multimedia	1		
54.	Must support Reliable Multicast to Unicast conversion to maintain video quality at AP level	1		
55.	Must support QoS and Video Call Admission Control capabilities.	1		
56.	Access Point should be 802.11 DFS certified	1		
57.	AP model proposed must be able to be both a client-serving AP and a monitor-only AP for Intrusion Prevention services.	1		
58.	Access Point should have integrated Antenna.	1		
59.	Real Time monitoring of links. Real time fetching of reports per access point	2		M
60.	APN-wise report generation in the industry standard formats (.csv, excel, pdf, pipe separated etc.)	1		
61.	Solution must provide a centralized dashboard application/Web URL to fetch all details/reports/logs at one place.	2		M

62.	Sensors should test the DNS & DHCP server connectivity & response. Solution should provide a network summary in terms like busiest day in month basis on client count, APP usage, radio throughput, app count, interference, traffic etc.	1		
63.	Automatic failover should happen at access points level & also Controller	1		
64.	Automatically shift to adjacent access points if the load is high on particular access points	1		
65.	Secure Tunnel between Wireless access point and wireless controller	1		
Wireless Troubleshooting and Sensors				
66.	Solution should include Adaptive Wireless Intrusion Prevention System (WIPS). WIPS solution should provide compliance and audit reporting.	2		M
67.	The solution should provide SEBI to view all access points deployed across SEBI locations and track Wi-Fi tags, rogue APs, rogue devices, Wi-Fi interferers, and BLE beacons in real-time.	2		M
68.	For proactive wireless troubleshooting bidder should quote wireless Assurance solution with sensors (for both 2.4 GHz and 5 GHz) and required appliance/software.	2		M
69.	It should provide network health Solution and trend to highlight status of device health like CPU, Memory utilization, interface availability etc. with remediation suggestions. It should highlight top AP by client count, Top AP with highest interference etc. Sensor should have test option to test local gateway connectivity and to test connectivity to RADIUS server.	1		
70.	Solution should provide wireless client onboarding events like Association failure, Authentication failure, IP address failure, Excessive On-boarding time, Excessive authentication time, Excessive IP addressing Time.	2		M
71.	The solution should provide you a Solution to view all access points deployed across your locations and track Wi-Fi tags, rogue APs, rogue devices, Wi-Fi interferers, and BLE beacons in real-time.	1		
72.	For proactive wireless troubleshooting bidder should quote wireless Assurance solution with sensors and required appliance/software.	1		

73.	Sensor should be able to do connectivity test from location to SSID. They should test connectivity by associate, authenticate and getting an IP address. There should be option to schedule the tests for proactive 1monitoring.	1		
74.	Sensors should be dedicated sensors to able to provide the insights for both 2.4 and 5ghz.	1		
75.	Sensors should test the DNS, DHCP, RADIUS server connectivity and report if failed to get an IP address. Sensor should report if there is slow response.	1		
76.	The solution should provide network health and trend to highlight status of device health like CPU, Memory utilization, interface availability etc. with remediation suggestions. It should highlight top AP by client count, Top AP with highest interferance etc.	1		
77.	WIPS should detect and protect an Ad-hoc connection when a connected user forming a network with other system without an AP or try enabling bridging between two interface	2		M
78.	WIPS should detect if a user try to impersonate a management frame.	1		
79.	WIPS should detect and take appropriate containment action if a smartphone user using tethering to connect other device.	2		M
80.	WIPS solution should provide compliance and audit reporting.	1		
81.	WIPS solution should provide rogue visualization with location intelligence on map.	1		
82.	WIPS functionality should be available on both centralize and distributed traffic forwarding mode from AP.	1		
83.	WIPS solution should provide global alarm consolidation for ease of use.	1		
84.	WIPS solution should provide complete threat library with location intelligence and historical rogue reporting.	1		

10.2.10. Video Conferencing Functional & Technical requirements:

Sr. No.	Description /Specification	Score	Compliance (Yes/No)	Remarks
	Call Features for HDVC end points			
1.	The System should be rack mountable appliance with minimum 1U size or more. The System should be supplied with necessary power cards, cables, bracket accessories and other appropriate accessories. The system should support registration of H.323 and SIP devices and all the required licenses to be included as part of solution.	2		M
2.	The system should Support for Automatic call routing using H.323/SIP, Support Active Directory integration and enable minimum at least 1+6 multi-party connections on each video end point device.	2		M
3.	The Large conference room video conferencing units should support multiple dial plans like IP to IP and SIP Calling and integrating with Software based video applications.	1		
4.	The Mid-sized room video conferencing units should support at least HD 720p (1080p and 4 K) resolution from day one	1		
5.	The solution must be able to share content at any time during a call either with another client or with hardware-based endpoint.	1		
6.	Should support video calls in 720p and 1080p and 4 K resolution from day one, and all the required licenses to be included as part of solution.	2		M
7.	Web-based real-time access for network administration. Call logging and diagnostics.	1		M
Software based video conferencing features				
8.	The software based video conferencing solution should provide collaboration facility for users to interact using application based group chat,	1		M

	collaboration, data sharing, Audio and Video calling, Join and schedule video conferencing meetings etc.			
9.	Schedule video conferencing using web based URL and Desktop and Mobile application as well, Recording meeting, live streaming, mute, unmute and other common features.	1		M
10.	SIP invite feature to join the conference by Video conferencing end points.	1		M
11.	Software based conferencing solution (OEM 1) should have SEBI's division based licenses which can have at least 1000 participants in a meeting.	1		
12.	Software based conferencing solution (OEM 1) should have SEBI's individual licenses which can have at least 100 participants in a meeting.	1		
13.	Software based conferencing solution (OEM 2) for Webinar should have 30 licenses which can have at least 1000 participants in a meeting.	1		
14.	Software based conferencing solution (OEM 2) should have features of webinar like vote, polling, hard mute, bulk mute/unmute, setting up panellist, host, cohost, attendee, generate webcast (Live streaming) link etc.	1		

10.2.11. Software Defined Network Solution Functional & Technical requirements:

Sr. No.	Required Minimum Specification	Score	Compliance (Yes/No)	Remarks
1.	Software defined solution for centralized configuration, management and monitoring. The solution should support software defined automation and network device life-cycle management. Solution should be capable of plug and play configuration and template based network provisioning. Solution should support advanced wireless troubleshooting using wireless sensors.	2		M
2.	The solution should have Zero Touch provisioning (Plug and Play) when connected in SIT-NET. Solution should have Automated network devices on-boarding. The system should allow for plug and play installation of network devices without requiring any manual configuration.	2		M
3.	Identifying and monitoring Network Topology within site location.	2		M
4.	MACsec based Encryption of network traffic between switch to switch within SIT-NET and must support.	2		M
5.	System should support preferred version of software image and highlight devices deviating from preferred version. System should support GUI based upgrade of switches deployed in SIT-NET.	2		M
6.	Centralized Management Solution should able to configure, manage and monitor routers, switches, Wireless controllers, APs	1		
7.	It should able to discover network devices and map them into topology based on IP address, CDP or LLDP, IP device tracking and ARP entries, SNMP etc.	1		
8.	It should periodically scan the network and keep the network inventory up to date and provide details on device serial number, model, software image, network role and location, etc. It should allow grouping of devices based on device type, Software image, location etc.	1		
9.	It should provide hierarchical network topology where devices are mapped to floor, building, area, etc.	1		
10.	Solution should allow network profile based setting to map common services like DHCP,	1		

	AAA, SNMP, IP address pool etc. For wireless, It should allow to create SSID and RF profiles to automate settings at multiple locations.			
11.	It should allow to create CLI or model based template which can be pushed to devices.	1		
12.	In case of device failure, It should help to automate replacement like software restoration, license restoration, updaing inventory etc.	1		
13.	It should provide high level summary view on devices and client on the network, top 10 global issues and should allow admin to expand view on sites, devices, client, topology etc.	1		
14.	Solution should support Health score and Issue priority settings	1		
15.	Solution should be able to check configuration compliance (running config vs startup config)	1		
16.	Solution should support North bound REST APIs to integrate with third party software	1		
17.	Solution should support role based access control. (RBAC)	1		
18.	It should support backup and restore capability	1		
19.	Health Score: The system should support identifying and reporting Top 10 issues and health score of network devices. The system should provide workflow to Troubleshoot the network issues like slowness/access issues.	1		

10.2.12. Network Devices Functional & Technical Requirements

Sr.No.	**Description /Specification**	**Score**	**Compliance (Yes/No)**	**Remarks**
Core switches				
1.	Multi-slot chassis-based switch with at least 6 slots. Minimum 4 slots for interface/payload line cards and 2 slots for switch processors	2		M
2.	The proposed switch will have redundant CPUs from day-1. Platform should integrate with centralized control and management platform from Day 1. Should support Non-Stop	2		M

	Forwarding and Stateful Switchover to ensure information between supervisor engines are fully to allow the standby supervisor engine to take over in subsecond time if the primary supervisor fails.			
3.	Switch should support In Service Software Upgrade (ISSU) with two chassis configured in HA mode to provide an upgrade of the entire chassis or an individual task/process without impacting hardware forwarding.	2		M
4.	Fully populated redundant Power supply from day 1 to support N:N redundancy mode. Switch should support field replaceable components such as Supervisor, Line cards, Power-supply, and Fan trays.	1		
5.	Chassis should support multiGigabit interfaces.	2		M
6.	Platform should integrated with centralized control and management platform from Day 1.	1		
7.	Switch support Single Operating System binary image for all Layer-2 and Layer-3 switch models proposed as part of the design	1		
8.	Switch should have capabilities to seamless upgrade/replacement (without interrupting services) for modular interfaces.	1		
9.	Switch should support IEEE Standards of Ethernet: IEEE 802.1D, 802.1s, 802.1w, 802.1x, 802.3ad, 802.3x, 802.1p, 802.1Q, 802.3, 802.3u, 802.3ab, 802.3z & 1588.	1		
10.	Switch must have functionality like static routing, RIP, PIM, OSPF, VRRP, PBR and QoS features from Day1	1		
11.	Switch must have advance Layer 3 protocol like BGPv4, BGPv6 , MPLS, VRF, VXLAN, IS-ISv4, OSPFv3, MP-BGP	1		
12.	Switch must support Netflow, SPAN, Model-Driven Telemetry and automation features like NETCONF, RESTCONF, YANG.	1		
13.	Switch should support 802.1x authentication and accounting, IPv4 and IPv6 ACLs and Dynamic VLAN assignment on hardware for all ports.	1		
14.	Communication between switch-to-switch should support line-rate encryption as per industry standard IEEE 802.1AE (MACsec)	2		M
15.	During system boots, the system’s software signatures should be checked for integrity. System should be capable to understand that system OS are authentic and unmodified, it should have cryptographically signed images to provide assurance that the firmware & BIOS are authentic.	1		

16.	Switch must support Netflow/Sflow, SPAN, Model-Driven Telemetry and automation features like NETCONF/RESTCONF/YANG or Rest API. OS should have support for Management automation vis Netconf/Yang or equivalent.	1		
17.	Switch must have advance Layer 3 protocol like BGPv4, BGPv6, MPLS, VRF, VXLAN, IS-ISv4, OSPFv3, MP-BGP	1		
18.	The Switch should support IPSLA and VRF features	1		
19.	Switch should support IPv6-logo-ready certified	1		
20.	Switch / Switch’s Operating System should be tested for EAL 2/NDPP or above under Common Criteria Certification.	1		
21.	Centralized Management Solution should able to configure, manage and monitor routers, switches, Wireless controllers, APs	1		
22.	It should provide zero touch provisioning for new device installation	1		
23.	It should able to discover network devices and map them into topology based on IP address, CDP or LLDP, IP device tracking and ARP entries, SNMP etc.	1		
24.	It should periodically scan the network and keep the network inventory up to date and provide details on device serial number, model, software image, network role and location, etc. It should allow grouping of devices based on device type, Software image, location etc.	1		
25.	It should provide centralized software image management for network devices like routers, switches and wireless.	1		
26.	Solution should support definition of preferred software image and highlight device software image is not matching preferred image	1		
27.	It should provide hierarchical network topology where devices are mapped to floor, building, area, etc.	1		
28.	Solution should allow network profile-based setting to map common services like DHCP, AAA, SNMP, IP address pool etc. For wireless, It should allow to create SSID and RF profiles to automate settings at multiple locations.	1		
29.	It should allow to create CLI or model-based template which can be pushed to devices.	1		
30.	In case of device failure, It should help to automate replacement like software restoration, license restoration, updating inventory etc.	1		

31.	It should provide high level summary view on devices and client on the network, top 10 global issues and should allow admin to expand view on sites, devices, client, topology etc.	1		
32.	Solution should support Health score and Issue priority settings	1		
33.	Solution should be able to check configuration compliance (running config vs startup config)	1		
34.	Solution should support North bound REST APIs for device discovery, inventory, software upgrade, device health monitoring to integrate with third party software	1		
35.	Solution should support role-based access control. (RBAC)	1		
36.	It should support backup and restore capability	1		
Access Switches				
37.	Switch should be 1U and should be rack mountable in standard 42 rack. Switch should have one power supply module installed from day 1 and should support internal field replaceable redundant power supply.	2		M
38.	Switch should have minimum 2 GB RAM and 2 GB Flash. Switch must have functionality like static routing, and QoS features from Day1.	1		
39.	Switch should have dedicated slot for modular stacking, in addition to minimum 4 uplink ports. Should support for minimum 48 Gbps of stacking throughput with 8 switches in single stack.	2		M
40.	Switch should support multigigabit platform to connect in same stack for future requirement	2		M
41.	Switch should support common Operating System binary image for all Layer-2 and Layer-3 switch models proposed as part of the design	1		
42.	Switch should be integrated with centralized control and management platform from Day 1.	1		
43.	Switch should have non-blocking switching fabric. (176 Gbps switching capacity for model having 48 downlink ports)	1		
44.	Switch should have minimum 16K MAC Addresses and 250 active VLAN. Switch should support 128 or more MSTP Instances.	1		
45.	Switch should have 6MB or more packet buffer.	1		
46.	Switch should support SSO and sub-sec failover on stacked switches.	1		
47.	Switch should support IEEE Standards of Ethernet: IEEE 802.1D, 802.1s, 802.1w, 802.1x,	1		

	802.3ad, 802.3x, 802.1p, 802.1Q, 802.3, 802.3u, 802.3ab, 802.3z.			
48.	Switch must support Netflow/Sflow, SPAN, Model-Driven Telemetry and automation features like NETCONF/RESTCONF/YANG or REST API. Switch should support management features like SSHv2, SNMPv2c, SNMPv3, NTP, RADIUS and TACACS+ .	1		
49.	Switch should have 802.1p class of service, marking, classification, policing and shaping and eight egress queues.	1		
50.	Switch should support IPv6 Binding Integrity Guard or equivalent, IPv6 Snooping, IPv6 RA Guard, IPv6 DHCP Guard, IPv6 Neighbor Discovery Inspection and IPv6 Source Guard.	1		
51.	Switch should support 802.1x authentication and accounting, IPv4 and IPv6 ACLs and Dynamic VLAN assignment and MACsec on hardware for all ports.	1		
52.	Switch must have the capabilities to enable automatic configuration of switch ports as devices connect to the switch for the device type.	1		
53.	Switch should have 48 nos. 100/1000 Base-T ports and additional 4 nos. SFP based uplinks ports.	1		
54.	All ports should support PoE (802.3af) and PoE+ (802.3at). Minimum PoE budget must be 370W for 24port switch and 740W for 48port switch	1		
55.	Switch should support IPv6-logo-ready certified or IPv6 ready. Switch should conform to UL 60950 or IEC 60950 or CSA 60950 or EN 60950 Standards for Safety requirements of Information Technology Equipment. Switch should conform to EN 55022 Class A or CISPR22 Class A or CE Class A or FCC Class A Standards for EMC (Electro Magnetic Compatibility) requirements.	1		
56.	Switch / Switch's Operating System should be tested for EAL 2/NDPP or above under Common Criteria Certification or FCC certified.	1		
Server Farm Switches				
57.	Switch should be 1U and rack mountable in standard 19" rack. Switch should support internal hot-swappable Redundant Power supply and fans from day 1.	1		
58.	Switch should be having dual power supply and should have integrated redundant hot swappable power supply. Switch should have redundant hot swappable fans.	2		M
59.	Switch should have minimum 8 GB RAM and 8 GB Flash.	1		

60.	Switch should have 48x1/10 GE SFP based port + 4x40 GE QSFP ports	2		M
61.	Switch should support Virtual Switching Sub-system (VSS) or equivalent feature that allows link from 2 different physical switches to appear as a single port channel.	2		M
62.	Switch should support minimum 3 Tbps switching bandwidth.	1		
63.	Switch shall have minimum 32K MAC Addresses and 1000 active VLAN.	1		
64.	Should support minimum 32K IPv4 routes or more and 16K IPv6 routes or more	1		
65.	Switch should have 8K or more multicast routes.	1		
66.	Switch should support atleast 64K flow entries	1		
67.	Switch should support 128 or more STP Instances.	1		
68.	Switch should have 16MB or more packet buffer.	1		
69.	Switch should support IEEE Standards of Ethernet: IEEE 802.1D, 802.1s, 802.1w, 802.1x, 802.3ad, 802.3x, 802.1p, 802.1Q, 802.3, 802.3u, 802.3ab, 802.3z & 1588v2.	1		
70.	Switch must have functionality like static routing, RIP, PIM, OSPF, VRRP, PBR and QoS features from day1. Switch must have advance Layer 3 protocol like BGPv4, BGPv6, MPLS, VRF, VXLAN, IS-ISv4, OSPFv3, MP-BGP from day1. Switch should support management features like SSHv2, SNMPv2c, SNMPv3, NTP, RADIUS and TACACS+.	1		
71.	Switch shall have 802.1p class of service, marking, classification, policing and shaping and eight egress queues.	1		
72.	Switch should support IPv6 Binding Integrity Guard, IPv6 Snooping, IPv6 RA Guard, IPv6 DHCP Guard, IPv6 Neighbor Discovery Inspection and IPv6 Source Guard.	1		
73.	Switch should support 802.1x authentication and accounting, IPv4 and IPv6 ACLs and Dynamic VLAN assignment and MACSec on hardware	2		M
74.	Switch must have the capabilities to enable automatic configuration of switch ports as devices connect to the switch for the device type.	1		
75.	Switch should conform to UL 60950 or IEC 60950 or CSA 60950 or EN 60950 Standards for Safety requirements of Information Technology Equipment. Switch should conform to EN 55022 Class A/B or CISPR22 Class A/B or CE Class A/B or FCC Class A/B Standards for EMC (Electro Magnetic Compatibility) requirements.	1		

76.	Switch / Switch's Operating System should be tested for EAL 2/NDPP or above under Common Criteria Certification. Switch should support IPv6-logo-ready certified	1		
Link Load Balancer				
77.	Solution should be dedicated, purpose built, On Demand upgradable & Appliance based solution.	1		
78.	The proposed solution should be purpose build ASIC based hardware appliance	1		
79.	System should have 2X10 G SFP+ Ports & 8X1 G Copper Ports, support from day one.	1		
80.	Should have minimum 8 GB memory and upgradable to 16 Gb of Memory.	1		
81.	hardware should have dual power supply	2		M
82.	Solution should be market proven link load balancing solution from last 5 years.	1		
83.	Solution should be market proven link load balancing and ability to resolve DNSSEC.	1		
84.	System should support inbound and outbound load balancing.	2		M
85.	System should support at least 8-10 internet/intranet links to load balance.	2		M
86.	System should support multi path health monitoring to monitor the link status.	2		M
87.	Should support server side web compression and proximity based LLB	1		
88.	Selection of shortest path to destination based on load/hops/response time.	1		
89.	Should support static & dynamic proximity based outbound as well as inbound load balancing.	1		
90.	Solution should support traffic shaping/Bandwidth Management from Day 1.	1		
91.	Offered product should be IPv6 Ready.	2		M
92.	Should have predefined health check on protocols like HTTP,SMTP,POP3,DNS.Ping,FTP,SNMP etc.	1		
93.	Should support routing protocols RIP, OSPF and BGP to participate in Dynamic routing	1		
94.	Should Support VRRP based failover	1		
95.	Should support transparent failover between 2 devices (if any)	1		
96.	Should support Client table Mirroring from Active to Backup Device	1		
97.	Should provide GUI interface for configuration & reporting	2		M
98.	Should provide HTTP / HTTPS interface management	2		M
99.	Should provide SSH / Telnet / CLI interface	1		

100.	Should support SNMP V3	2		M
101.	Link Load Balancer should support IP base, user base, URL base traffic and bandwidth reservation	2		M
Network Rack Specifications For Data Centre (Rack Unit)				
102.	42U Floor Mount Rack 800MM X 1000MM Rack with fixing with ground kit., 3 X 2" X 2 gland for fiber entry and 3 "X 2" X 2 Glands for copper entry (Color-Black)ft	2		M
103.	Door Steel HEX-PRF, 800W, Door Steel DUAL HEX-PRF 800W 42U	1		
104.	Castor Heavy duty 250KG Per BRAKE	1		
105.	Fans 90 CFM 230 VAC	1		
106.	1Ph 230V, 16A, Zero U, Standard Horizontal Rack Mount Power Distribution Unit with 6 x Indian Round Pin socket, 5/15A, 16A MCB, 3.6 KVA rating, 3 meter Power cord with Industrial Plug	1		
107.	HARDWARE FRONT PANEL MTG PKT OF 20 each	1		
108.	Earthing Kit	1		
109.	Shelf Heavy Duty 725MM	1		
110.	Blanking Panel 19 " 1U and 2U ABS	1		
111.	Rack PDU 2G Metered ZeroU, 32A, 230V, (36) C13 & (6) C19(single phase) 3 meter Power cord with Industrial Plug	1		

10.2.13. Patch Management Solution Functional and Technical Requirements

Sr.No.	Description / Specification	Score	Compliance (Yes/No)	Remarks
General Features				
1.	The solution should be integrated with PIM solution, provide two-factor authentication and role-based access controls.	2		M
2.	Testing: The solution should be able to apply the patches to a representative sample of assets in SIT-NET. The testing will ensure that the patches will not cause issues in SEBI's production environment.	2		M
3.	Create custom deployments: The solution should have the ability to create custom groups, such as by operating system, by department, by java version or as per requirement. The solution should be able to deploy a patch or update to a specific group of computers (Example: There might be an emergency patch to Windows 10 computers or computers on a specific version of java etc.)	1		
4.	Pre-Built Packages and 3rd Party Patching: The solution should provide pre- built packages such as, adobe reader, java, flash, browser updates. The pre-built packages should be configured to silently install to save time. The solution should Detect, Report and Patch most used applications such as adobe, java, browsers, zip programs, Windows and Microsoft office.	1		
5.	Patch Status and Alert Generation: The solution should provide real-time patch status and enable to quickly see how many systems are unpatched, having missing updates and systems that have failed. The solution should be capable to generate alerts on new patch update availability or on finding vulnerability on patches for certain threshold timeline.	2		M
6.	Supports Windows 10 Feature Pack Deployment to upgrade Windows 7, Windows 8, Windows 8.1 and Windows 10 OS to latest version of Windows 10 OS	2		M
7.	Scheduled or On-Demand Patch Deployment	2		M

	And Controls System Reboot through Reboot Policy and Reduce Bandwidth Utilization through Master Agent.			
8.	Software Installation (MSI and Silent Executables), Software Un-installation (MSI and Silent Executables).	2		M
Reports				
9.	**Detailed Reports:** The solution should provide detailed reports including but not limited to the following- Top vulnerable systems, Top missing patches, systems that need reboot to complete patch update, and being able to report on specific patches, Category wise filter and sorting to generate report on device version, device category, device OEM name, etc.	1		
10.	The solution should provide history of the patches update along with the reports, scheduling of Reports for automatic Report generation and emailing of the same, ready to use Dashboards along with facility to create Custom Dashboards, Custom Report Builder, Export Reports to Excel and PDF Files, Easy generation of compliance and non-compliance reports	1		
Offline Compliance				
11.	Retry to offline machines: In cases where during the patch update, the user machine is offline, the solution should auto retry once that machine is online. Once the offline machine gets online, the patch should get updated and the same should be indicated in the latest report as well.	2		M
12.	Patch update details: The solution should provide the date and time on which the machine(s)/endpoint(s) has got updated with latest patches.	2		M
13.	The solution should provide full hardware and software inventories and solution should be able to create custom schedules to specific computers or groups of endpoints. Master License inventory to hold the existing licenses purchased for various devices in SIT-NET project.	2		M
Remote Access				
14.	The solution should Remotely manage all endpoint devices without interrupting end-users through a robust suite of remote tools and solution should directly take control of devices with remote access.	1		

Automation				
15.	Auto Discovery feature for devices which are newly added in SIT-NET with configurable discovery interval.	1		
16.	Automatic patch deployment: The solution should have the option to auto deploy when new patches are available. Automatic or Manual Approval of Missing Patches, Auto Device Type Categorization	1		
End User Data Gathering				
17.	Collects End User Data using Custom Data Collection Forms, The Data Input Fields in the Custom Form can be customized as per the requirements, Supports sending On-Screen Announcements to the End User System, The Custom Forms and Announcements can be published to selected nodes for a specific time period.	2		M
18.	The solution should be able to gather the endpoint devices data for analysis and monitoring purpose like CPU utilization, RAM size, Windows version, Antivirus installation and patch version, list of software installed on endpoints etc.	2		M
Blacklisting Patch update				
19.	Blacklisting Software Usage Blocking based on Software MSI File Name, Executable File Name and Executable Checksum, Automatic Uninstallation of Blacklisted Software.	1		
Hardware and Software Change Tracking				
20.	Maintains Hardware and Software Change Logs, Change Analysis through Change Log Dashboard, Integration and Linking of Changes to Service Desk Tickets, Alarms and Email and SMS Alerting on Meaningful Changes using Alarm Unification.	1		

Appendix VII: Responsibility matrix

Sl. No.	Activity	Bidder	SEBI
1.	Study of Existing SEBI Network & Infrastructure	√	
2.	Submission of the detailed document with architecture, flow diagram	√	
3.	Installation of SIT-NET Solution	√	
4.	Maintenance & Management of existing infra under AMC & infrastructure during implementation	√	
5.	Onsite FMS support for entire SIT-NET network (DC Infrastructure, Regional and Local office Connectivity & DR infrastructure).	√	
6.	Call logging & Ticket management & tracking the same till resolution	√	
7.	Performance testing	√	√
8.	Third party Software maintenance	√	
9.	Security Testing	√	√
10.	UAT	√	√
11.	VAPT	√	
12.	Infrastructure monitoring and submission of reports	√	
13.	Manage and maintain an inventory list, detailing all key characteristics of the inventory	√	
14.	Approve all documentations & list		√
15.	Submission of security Reports	√	
16.	Support during internal audits	√	
17.	SLA management and submission of its report	√	
18.	Project Management and Monthly Project Meeting	√	
19.	Provide and maintain a single point of contact for the reporting and tracking of Incidents.	√	
20.	Record, track, manage and resolve all Incidents received.	√	
21.	Provide service desk problem determination methods, minor problem resolution procedures, cause determination scripts, training and certification testing to the service desk	√	
22.	Report on Incidents within established time frames.	√	
23.	Perform root cause analysis for problems as requested by SEBI or in accordance with agreed Industry Standards	√	

24.	Produce root cause analysis report with recommendations to prevent reoccurring events.	√	
25.	Approve or escalate root cause analysis recommendations		√
26.	Implement root cause analysis recommendations as approved by SEBI and as requested/assigned for respective areas of service responsibility and providing support thereof.	√	
27.	Maintaining and testing DC, DR activity. Participating in periodic DR Drill of SEBI network as well as in other SEBI projects.	√	√
28.	Licensing, Warranties and Maintenance Management	√	√
29.	Perform system administration activities	√	
30.	Provide hardware, patch management, software installation and maintenance support.	√	
31.	Perform upgrades and maintain Software as required consistent as per OEM's Standard guidelines	√	
32.	Review and approve all new versions, upgrades, updates and customizations.	√	
33.	Maintain all License Usage Report per system wise	√	
34.	Install initial versions, new versions, upgrades, updates and customizations of Software.	√	
35.	Training	√	
36.	Provide Professional Comprehensive Training with Certification to at nominated employees of SEBI	√	
37.	Provide on-going knowledge transfer which will facilitate skills progression.	√	
38.	Provide training on new technology, functionality and Major Enhancements.	√	
39.	Security	√	
40.	Define security policy and guidelines	√	√
41.	Integration with NOC SOC solutions	√	
42.	Verification of Network devices integration with SOC-NOC devices/solutions	√	
43.	Integration of Network devices with SEBI's other solutions/components	√	
44.	Verification of Network devices with SEBI's other solutions/components	√	
45.	Define security requirements in accordance with the security policy and select suitable security solutions	√	√
46.	Manage, maintain, support and co-ordinate security solutions.	√	
47.	Preventive Maintenance	√	

48.	Installation and troubleshooting of solution components at end user’s machines/desks/locations	√	
	Monitoring of network and generate periodic and ad-hoc MIS reports for SEBI	√	

Appendix VIII: Performance Bank Guarantee

WHEREAS
M/s. (name of Bidder), a company registered under the Companies Act, 1956, having its registered and corporate office at (address of the Bidder), (hereinafter referred to as "our constituent", which expression, unless excluded or repugnant to the context or meaning thereof, includes its successors and assigns), entered into an Agreement dated …….. (Hereinafter, referred to as "the said Agreement") with you (Securities and Exchange Board of India) for design, development, implementation and maintenance of SIT-NET project at SEBI, as detailed in the said Agreement.

We are aware of the fact that in terms of sub-para (…), Section (…), Chapter (…) of the said Agreement, our constituent is required to furnish a Bank Guarantee for an amount Rs…….. (In words and figures), being *<Value of Performance Bank Guarantee in Percentage>* of the Agreement Price of Rs. … (In words and figures), as per the said Agreement, as security against breach/default of the said Agreement by our Constituent.

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

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

i. In the event of our constituent committing any breach/default of the said Agreement, which breach/default has not been rectified within a period of thirty (30) days after receipt of written notice from you, we hereby agree to pay you forthwith on demand such sum/s not exceeding the sum of Rs…… (In words and figures) without any demur.
ii. Notwithstanding anything to the contrary, as contained in the said Agreement, we agree that your decision as to whether our constituent has made any such default/s / breach/es, as aforesaid and the amount or amounts to which you are entitled by reasons thereof, subject to the terms and conditions of the said Agreement, will be binding on us and we shall not be entitled to ask you to establish your claim or claims under this Performance Bank Guarantee, but will pay the same forthwith on your demand without any protest or demur.
iii. This Performance Bank Guarantee shall continue and hold good till the completion of the warranty period for the 'Total Solution' i.e. (date), subject to the terms and conditions in the said Agreement.
iv. We bind ourselves to pay the above said amount at any point of time commencing from the date of the said Agreement until the completion of the warranty period for the Total Solution as per said Agreement.

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

vi. In order to give full effect to the guarantee contained herein, we (name and address of the bank), agree that you shall be entitled to act as if we were your principal debtors in respect of your claims against our constituent. We hereby expressly waive all our rights of surety ship and other rights, if any, which are in any way inconsistent with any of the provisions of this Performance Bank Guarantee.

vii. We confirm that this Performance Bank Guarantee will cover your claim/s against our constituent made in accordance with this Guarantee from time to time, arising out of or in relation to the said Agreement and in respect of which your claim is lodged with us on or before the date of expiry of this Performance Guarantee, irrespective of your entitlement to other claims, charges, rights and reliefs, as provided in the said Agreement.

viii. Any notice by way of demand or otherwise here-under may be sent by special courier, registered post or other electronic media to our address, as aforesaid and if sent by post, it shall be deemed to have been given to us after the expiry of 48 hours when the same has been posted.

ix. If it is necessary to extend this guarantee on account of any reason whatsoever, we undertake to extend the period of this guarantee on the request of our constituent under intimation to you (Securities and Exchange Board of India).

x. This Performance Bank Guarantee shall not be affected by any change in the constitution of our constituent nor shall it be affected by any change in our constitution or by any amalgamation or absorption thereof or therewith or reconstruction or winding up, but will ensure to the benefit of you and be available to and be enforceable by you.

xi. Notwithstanding anything contained herein-above, our liability under this Performance Guarantee is restricted to Rs…… (in words and figures) and shall continue to exist, subject to the terms and conditions contained herein, unless a written claim is lodged on us on or before the aforesaid date of expiry of this guarantee.

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

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

Notwithstanding anything contained herein:

i. Our liability under this Performance Bank Guarantee shall not exceed Rs. …. (in words and figure) ;
ii. This Performance Bank Guarantee shall be valid only up to …….. (date, i.e. completion of warranty period for the Total Solution) ; and
iii. We are liable to pay the guaranteed amount or part thereof under this Performance Bank Guarantee only and only if we receive a written claim or demand on or before …. (Date i.e. completion of the warranty period for the Total Solution).

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

Dated ……………………. this ……….. Day …………. <*YEAR*>.

Yours faithfully,

For and on behalf of the …………… Bank,

(Signature) Designation
(Address of the Bank)

Note:
a. This guarantee will attract stamp duty as a security bond under Article 54(b) of the Mumbai Stamp Act, 1958.
b. A duly certified copy of the requisite authority conferred on the official/s to execute the guarantee on behalf of the bank should be annexed to this guarantee for verification and retention thereof as documentary evidence in the matter.

Appendix IX: Draft Master Service Agreement

The following are the general terms and conditions proposed to be included in the Agreement. However, these terms and conditions are not exhaustive and SEBI reserves the right to add, delete, modify or alter all or any of these terms and conditions in any manner, as deemed necessary by SEBI. SEBI also reserves the right to add, delete, modify or alter all or any of these terms and conditions in any manner, subject to any law of the land or directives issued by Government of India or the Central Vigilance Commission from time to time as the case may be.

The Solution Provider, selected for setting up of SIT-NET, will have to enter into an agreement directly with SEBI. The agreement shall contain various terms and conditions relating to payment, delivery, installation & operationalization, training, commissioning & acceptance, support during periods of warranty & maintenance, liability and penalty due to delay in performance responsibilities, etc. All the diagrams, drawings, specifications and other related literature & information, provided by the Solution Provider under the total solution and agreed to by SEBI, shall also form a part of the agreement.

The bill of material containing item-wise details in respect of all products, covered under the SIT-NET solution , offered by the Solution Provider, must be furnished along with the prices thereof, as per the terms and conditions contained in this document. The Solution Provider shall undertake to ensure that the prices are reasonable and in the range of prices for similar / same products available in the market.

If any irregularity or any defect is detected anytime in respect of the above, SEBI shall have the right to take appropriate action against the Solution Provider, as deemed fit by SEBI.

All correspondences and other documents pertaining to the agreement/ contract shall be in English. The Agreement shall be governed and interpreted in accordance with the Indian laws.

12.1. Definitions

All definitions and meanings terms used in this Agreement will be as per the Request for Proposal ("RFP") document.

12.2. Standards

The goods/products/services, supplied under this Agreement shall conform to the standards mentioned in the Technical Specification or agreed between SEBI and the Solution Provider, and when no applicable standard is mentioned, the goods/products shall be supplied under the authoritative and appropriate international standards of the goods/products and such standards shall be the latest issued by the institutions concerned.

12.3. Prices

The price shall be exclusive of all taxes and SEBI will pay applicable taxes at the time of payment.

No escalation in price quoted shall be permitted for any reason whatsoever. Prices quoted shall be firm till the complete execution of the agreement including implementation, Warranty & Support, and AMC for *7.5 years.* Prices when quoted both in figures as well as in words have any discrepancy between the rates given in figures and in words, the rates given in words shall be considered.

12.4. Performance Bank Guarantee

The Solution Provider shall at his own cost and expense furnish within 30 (Thirty) business days from the effective date, an unconditional and irrevocable performance bank guarantee for <*Value of Performance Bank Guarantee in Percentage*> of Rs. __________/- (Rupees ____________ only) in favor of SEBI, from a scheduled commercial Bank towards the due and punctual performance and fulfillment of this agreement in the format prescribed in Appendix VIII of RFP. This Performance Bank Guarantee shall be valid till the end of the warranty Period under this Agreement.

The Performance bank guarantee shall contain a claim period of 3 (Three) months ("Claim Period") from the last date of validity ("validity date"). The performance bank guarantee may be discharged by SEBI upon being satisfied that there has been due performance of the obligations by the solution partner.

12.5. Taxes and Duties

1. The Successful Solution Provider shall be entirely responsible to pay all the taxes including but not limited to goods and services tax, corporate tax and income tax, duties, fee, toll, royalty tax, etc. in connection with the installation of the systems and the provisions of the services necessary for the successful implementation and maintenance of the supplied system.
2. Wherever the laws and regulations require deduction of such taxes at the source of the payment, SEBI shall effect such deductions from the payment due to the Solution Partner. The remittance of the amount so deducted and issuance of certificate for such deductions shall be made by SEBI as per the laws and regulations in force.
3. Any reduction/increase in taxes and duties affected on or after date of submission of bid up to date of successful completion of warranty shall be passed on to and borne by SEBI.

12.6. Project Plan and Acceptance Tests

The selected Bidder ("Solution Provider") shall provide a Project plan to SEBI within one week of the signing of the Agreement. This Project Plan shall detail the tasks that has to be carried out and completed on various scheduled dates including the acceptance testing. The Solution Provider shall submit weekly report on the progress of the project and also the status as on the scheduled date and actual date of each activity detailing any deviations to the SEBI's project manager. An Acceptance Test Plan ("ATP"), identifying the tests proposed to be conducted, along with Test scripts would be prepared and submitted to SEBI by the Solution Provider. The Project Plan and the ATP shall not be considered complete and final unless the same have been reviewed and accepted by SEBI.

The errors found during the Acceptance Testing by SEBI shall be promptly rectified by the Solution Provider. The Acceptance of all the goods or products as well as services under the Agreement shall be deemed to have taken place when the Solution Provider, in accordance with the agreement, has completed their supply, installation and successful commissioning and SEBI thereafter certified to the Solution Provider in writing the SEBI's acceptance of the Systems. The SEBI's acceptance certificate of the supplied goods/products shall in no way release the Solution Provider from any of its warranty obligations under the agreement.

12.7. Dispute Resolution

i. All disputes and differences of any kind, whatsoever, between the Solution Provider and SEBI, arising out of or in relation to the construction, meaning, operation or effect interpretation of the agreement, or breach thereof shall be settled amicably. If, however, the Parties are not able to resolve any dispute or differences amicably, the same shall be referred to the sole arbitrator if mutually agreed upon, failing which, one arbitrator to be appointed by each Party to the dispute, and the third arbitrator to be appointed by the two arbitrators and such arbitration shall be in accordance with the provision of the Arbitration and Conciliation Act, 1996, or any statutory modification or re-enactment thereof for the time being in force. The award made in pursuance thereof shall be binding on the Parties. The seat and venue of the arbitration shall be in Mumbai.

ii. The Solution Provider shall continue to work under the agreement during the arbitration proceedings unless otherwise directed by the Arbitrator or by SEBI in writing, or unless the matter is such that, in the opinion of the arbitrator/arbitrators, the works cannot possibly be continued until the decision of the arbitrator/arbitrators, as the case may be, is obtained.

12.8. Notices

i. Notice or other communications given or required to be given under this Agreement shall be in writing and shall be hand-delivered with acknowledgement thereof, or transmitted by pre-paid registered post by reputed courier to the address of the receiving party by the other in writing, provided such change of address has been notified at least 10 (ten) days prior to the date on which such notice has been given under the terms of this Agreement.

ii. Any notice or other communications shall be deemed to have been validly delivered on date of delivery if hand-delivered; if sent by registered post or by reputed courier, then on the expiration of 7 (seven) days from the date of posting. All notices, requests, demands and other communications under this agreement or in connection herewith shall be given to or made upon the respective parties as follows:

To SEBI :
CGM (ITD),
Securities and Exchange Board of India
SEBI Bhavan,
Plot No. C4-A, "G Block"
Bandra Kurla Complex
Bandra (East) - 400 051
India

To Solution Provider:
<address of Solution Provider>

to such other person or addresses as any of the Parties shall have notified to the others.

12.9. Confidentiality

a. The Solution Provider acknowledges that as a result of the Services that the Solution Provider is providing here-under, the Solution Provider may have access to the Confidential Information and proprietary (which shall include but not be limited to any business, commercial or financial information of SEBI or any information, documentation, data and other materials related to SEBI's business and operations) of SEBI that is or has been disclosed to the Solution Provider by SEBI and marked as confidential when disclosed in writing and when disclosed orally, identified as confidential at the time of disclosure and submitted in writing to the Solution Provider within 7 (seven) Business Days of such disclosure.

d. Confidential Information does not include information which:

(i) is publicly available at the time of its disclosure; or becomes publicly available following disclosure; or

(ii) is already known to or was in the possession of the Solution Provider prior to execution of this Agreement; or

(iii) is disclosed to the Solution Provider by a third party, which party is not bound by any obligation of confidentiality; or

(iv) is or has been independently developed by the Solution Provider without using the Confidential Information or deriving from the Confidential Information of SEBI;

(v) is required to be disclosed with the prior consent of SEBI.

(vi) is required to be disclosed pursuant to any requirement/ guidelines/ direction/ order issued by regulatory, government, statutory bodies/ authorities.

e. Similarly, SEBI agrees that during the course of this Agreement, SEBI may receive or come into possession of information that is confidential/proprietary to the Solution Provider (including but not limited to information relating to software, trade secrets, know-how/ technical data, research, products, software services, development, inventions, processes, engineering techniques, strategies, etc.) and that SEBI shall not disclose or divulge such confidential/ proprietary information of the Solution Provider to any third parties or make use or allow others to make use thereof either for its own benefit or for the benefit of others, directly or indirectly, and that the terms and conditions herein above set out with respect of the confidential information of SEBI, shall apply mutatis mutandis to the Solution Provider's confidential/ proprietary information.

f. The confidentiality obligations of the Parties herein shall continue for the term of this Agreement and for a period of 2 (two) years thereafter.

g. The Parties agree that they shall not permit the duplication or disclosure of Confidential Information of other Party, to any person (other than an employee, agent or representative of that Party who needs such information for the specific purpose of performance of obligations under this Agreement). Any document, other than this Agreement itself, shall remain the property of the disclosing Party and all copies thereof shall be returned to such disclosing Party on termination of this Agreement or upon earlier request by disclosing Party.

h. The receiving Party understands and acknowledges that the disclosure of, or failure to adequately protect Confidential Information of disclosing Party, would result in irreparable harm to disclosing party. In addition to monetary damages, disclosing Party shall be entitled to any and all equitable remedies, including but not limited to injunctive relief, in the event the receiving party discloses or fails to protect the Confidential Information.

12.10. Indemnities

a. The Solution Provider shall be liable to indemnify SEBI, at its own cost and expenses, against all losses/damages, which SEBI may suffer on account of violation by the Solution Provider of any or all national/international trade laws, norms, standards, procedures etc. in relation to provision of services and deliverable under this Agreement.

b. Each Party shall be solely responsible for and shall indemnify and keep SEBI, its employees, agents, officers and directors indemnified and harmless from and against all costs (including but not limited to litigation expenses and attorney's fees), expenses, losses, liabilities, fines, penalties, damages, claims, demands, actions or proceedings whatsoever for arising out :

   (i) any death or personal injury caused by any act or omission of the Solution Provider, its employees or agents;

   (ii) any third party claims for infringement of a copyright, patent, trademark or other intellectual property right of any third party including claims made by agents of the Solution Provider against SEBI for any breach committed by the Solution Provider in relation to such third parties;

   (iii) any claims arising out of the breach of any applicable laws by the Solution Provider, its employees or agents;

   (iv) any claims arising out of breach of the terms and conditions of confidentiality, non-disclosure, non-solicitation and related terms and conditions.

Notwithstanding the foregoing; Solution Provider shall not be obliged to indemnify SEBI if the claim mentioned therein arises out of any:

   (i) use of the services, deliverable, developed materials and other materials provided to SEBI by Solution Provider in a manner or purpose not intended by the Project Plan or against specific instructions of the Solution Provider, or

   (ii) use of the services, deliverable, developed materials and other materials provided to SEBI by the Solution Provider in conjunction with third party materials of services if the claim of infringement would not have arisen in the absence of such use, or

   (iii) use of the services, deliverable, developed materials and other materials provided to SEBI by the Solution Provider that are being designed or made to specifications to the order of SEBI, or

   (iv) if the infringement is occasioned by a modification to the services, deliverable, developed materials and other materials provided to SEBI by the Solution Provider.

c. SEBI will defend, indemnify and hold the Solution Provider harmless from and against all losses, damages or costs arising out of or resulting from any action by a third party against the Solution Provider that is based upon any claim that the possession or use of any material supplied by SEBI in connection with the Services under this Agreement infringe a patent, copyright or other proprietary right or violate a trade secret of such third party and or for any loss, injury, claim or damage resulting from any death or injury to any person or property of the Solution Provider arising out of the use or possession of the equipment or location of SEBI by the Solution Provider or its personnel.

12.11. Intellectual Property Rights

i. All Custom Software/customizations developed and furnished solely and exclusively for SEBI under this Agreement, shall be deemed a work made for hire, for the sole benefit of and belonging exclusively to SEBI. All rights, title and interest in and to such Custom Software/customizations and all copies thereof, in whatever medium (and including all Moral Rights thereto) throughout the world shall become owned exclusively by SEBl. Intellectual property and Source Code in the deliverables/software developed under this Agreement vest with SEBI upon the delivery and acceptance of deliverables and the receipt of payment by Solution Provider.

ii. The Solution Provider and its employees and agents expressly waive any and all moral rights in the Custom Software, and any elements thereof, created, performed, contributed or prepared by the Solution Provider and its employees and agents pursuant to this Agreement. SEBI shall have the exclusive right to obtain and hold in its own name, all the Intellectual Property Rights in such Custom Software.

iii. The Solution Provider shall give SEBI all reasonable assistance required to perfect the foregoing rights to the Custom Software/customizations, including (but not limited to) directing its employees to execute all applications for patents, trademarks, and/or copyrights, domestic and foreign, assignments and other papers necessary to secure and enforce rights related to any Custom Software.

iv. SEBIacknowledges that in performing Services under this Agreement, the Solution Provider may use the Solution Provider's proprietary materials including without limitation any software (or any part or component thereof) tools, methodologies, processes, ideas, know-how and technology or any improvements, enhancements, modifications or customization thereto (Solution Provider Pre-Existing IP).

v. Notwithstanding anything to the contrary contained in this Agreement, the Solution Provider shall continue to retain all the ownership rights, title and interests to all Solution Provider Pre-Existing IP and nothing contained herein shall be construed as preventing or restricting the Solution Provider from using Solution Provider Pre-Existing IP in any manner. To the extent that any Solution Provider Pre-Existing

IP or a portion thereof is incorporated or contained in a Deliverable under this Agreement, the Solution Provider hereby grants to SEBI a fully paid-up, irrevocable, non- exclusive, license for non -commercial use throughout the territory of India to access, replicate and use any Solution Provider Pre-Existing IP (in connection with the Deliverables and only as part of the Deliverables in which they are incorporated or embedded) which are (a) embedded in the Systems; or (b) necessary for the proper utilization of the SEBI SIT-NET, provided by the Solution Provider, including all inventions, designs and marks, embodied therein in perpetuity.

vi. The foregoing license does not authorize SEBI to :

- separate Solution Provider Pre-Existing IP from the Deliverable in which they are incorporated for creating a standalone product for marketing to others; or

- independently sell, lease, exchange, mortgage, pledge, license, sub license, assign or in any other way convey, transfer or alienate the Solution Provider Pre-Existing IP in favour of any person (either for commercial consideration or not (including by way of transmission), and/or reverse compile or in any other way arrive at or attempt to arrive at the source code of the Solution Provider Pre-Existing IP.

vii. Notwithstanding anything to the contrary set forth anywhere else in the RFP or the Agreement,, the Solution Provider shall not use any third party or the Solution Provider’s proprietary software in the implementation of the *SIT-NET* that is not available to SEBI in the market on reasonable commercial terms. The Solution Provider shall identify all software and hardware that is necessary for the proper performance of the SIT-NET clearly to SEBI prior to execution of this Agreement.

viii. All the Intellectual Property Rights in the third party software used in providing services including those forming part of or incorporated into the deliverables referred to above shall remain with the respective third party owners/ the Solution Provider's licensor and SEBI shall have user rights in accordance with end user license agreement (EULA) as applicable to use of such software.

ix. If any of the Deliverables is held or is believed by the Solution Provider to infringe third party intellectual property rights, the Solution Provider shall have the option, at its expense, to:

- modify the Deliverables so as to make it non-infringing, or
- obtain for SEBI a license to continue using the Deliverables.

12.12. Non Solicitation

Neither Party shall, without the consent of the other Party, employ or offer to employ (whether under a contract of service or under a contract for services) any person engaged or previously engaged by the other in a technical or managerial capacity in relation to the Project, during the subsistence of this Agreement and until a period of 24 (twenty four) months has expired after the termination or expiry of this Agreement.

For the avoidance of doubt, this restriction applies only to those employees who are connected with the Services performed under this Agreement. The clause does not prevent hiring based on responses by employees to public advertisement on any media that are not specifically targeted at the other Party's employees.

12.13. Force Majeure

i. The Solution Provider or SEBI shall not be responsible for delays or non-performance of any or all contractual obligations, caused by war, revolution, insurrection, civil commotion, riots, mobilizations, strikes, blockade, acts of God, epidemics, fire, flood, obstructions of navigation by ice of Port of dispatch, acts of Government or public enemy or any other event beyond the control of either Party, which directly, materially and adversely affect the performance of any or all such contractual obligations.

ii. Provided either Party shall immediately upon the occurrence of such a cause notify the other in writing of such causes. Unless otherwise directed by SEBI in writing, the Solution Provider shall continue to perform his obligations under this Agreement as far as possible, and shall seek all means for performance of all other obligations, not prevented by the Force Majeure event.

iii. In the event that the said Force Majeure event exceeds 15 (fifteen) days, SEBI shall have the option of terminating this Agreement upon reasonable advance written notice to the Solution Provider. However, the Solution Provider shall be entitled to receive payments for all services and deliverables rendered up to the date of the termination of this Agreement.

iv. If the performance in whole or in part or any obligation under this Agreement is prevented or delayed by any reason of Force Majeure for a period exceeding 90 (Ninety) days, either party may at its option terminate the contract without any financial repercussion on either side.

12.14. Publicity

i. Neither Party shall use any name, mark or symbol of the other in any publicity release or advertising material or for any other purpose whatsoever without securing the prior written consent of the other.

ii. Neither Party shall use the other Party's name or refer to the other Party directly or indirectly in any media release, public announcement or public disclosure relating to this Agreement or their subject matter, including in any promotional or marketing materials, customer lists, referral lists or business presentations without written consent from the other Party for each such use or release.

12.15. Waiver

No forbearance, indulgence or relaxation's by any Party at any time to require performance of any provision of this Agreement shall in any way affect, diminish or prejudice the right of such Party to require performance of that provision and any waiver by any Party or any breach of any provisions of this Agreement shall not be construed as a waiver or an amendment of the provisions itself, or a waiver of any right under or arising out of this Agreement.

12.16. Non-Assignment

The Solution Provider shall not assign in a manner contrary to the terms of this Agreement deal with all/ or any of its rights and obligations under this Agreement without the prior written consent of SEBI.

12.17. Severability

If any part, provision, representation or warranty of this Agreement is found to be invalid, illegal or unenforceable under the applicable law, then only that part, provision, representation or warranty shall be deemed to be deleted as if it never formed part of this Agreement as long as such invalidity, illegality or unenforceability subsists. However, the Parties shall, in good faith, strive to achieve the commercial meaning of such deleted part, provision, representation or warranty under the applicable law.

12.18. Shipment of Goods

i. The Solution Provider shall provide such packing of the goods/products as is required to prevent any damage or deterioration during transit to their final destination as indicated in this Agreement and SEBI shall not be responsible for any loss, misplacement of the goods or products. The packing, crating and/or boxing shall be sufficient to withstand, without limitation, rough or improper handling during transit and open storage. Packing case size and weights shall always take into consideration the remoteness of the goods'/products' final destination and the absence of heavy handling facilities at all points.

ii. Each case, packing or box shall be plainly marked to designated official of SEBI and will include inside a copy of the corresponding packing list identifying the contents, duly authenticated. All the goods or products under this Agreement shall be air freighted by the Solution Provider.

iii. The components of Total Solution as indicated in Annexure'__' to this Agreement shall be delivered to at the office of

Table 20: Addresses of SEBI offices

S/N	Office Type	Addresses
1	**Head Office (HO1)**	SEBI-HO-MUMBAI-SEBI BHAVAN I Plot No.C4-A, 'G' Block Bandra-Kurla Complex, Bandra (East), Mumbai - 400051
2	**Head Office (HO2)**	SEBI-HO2-MUMBAI-SEBI BHAVAN II Plot no. C-7, ‘G’ Block, Bandra Kurla Complex, Bandra(E), Mumbai - 400051, Maharashtra
3	**SEBI Office**	Mittal Court Office Mittal Court 'B' & 'C' Wing, 1st Floor, 224 Nariman Point, Mumbai - 400021
A		**NRO**
4	**Regional Office (RO)**	**Delhi** The Regional Director, NBCC Complex, Office Tower-1, 8th Floor, Plate B, East Kidwai Nagar, New Delhi-110023, Delhi
5	**Local Office (LO)**	**Chandigarh** SCO 127-128, First Floor, Sector 17C, Chandigarh - 160017, Chandigarh
6	**Local Office (LO)**	**Dehradun** 2nd Floor, GMVN Building, 74/1, Rajpur Road, Dehradun - 248001, Uttarakhand
7	**Local Office (LO)**	**Jammu** Hall No. 405-408, 4th floor, B-2, South Block, Bahu Plaza, Rail Head Complex Jammu, Jammu - 180014, Jammu and Kashmir
8	**Local Office (LO)**	**Lucknow** 3rd Floor, Eldeco Corporate Chambers-II, Vibhuti Khand, Gomti Nagar, Lucknow - 226010, Uttar Pradesh

9	**Local Office (LO)**	**Shimla** Shanti Vihar, Kasumpti, Shimla - 171009, Himachal Pradesh
B		**WRO**
10	**Regional Office (RO)**	**Ahmedabad** The Regional Director, Western Regional Office, Panchvati 1st Lane, Gulbai Tekra Road, Ahmedabad - 380006, Gujarat
11	**Local Office (LO)**	**Indore** 104-105, Satguru Parinay, Opposite C-21 Mall, A.B. Road, Indore - 452010, Madhya Pradesh
12	**Local Office (LO)**	**Jaipur** Ground Floor, Jeevan Nidhi 2, LIC Building, Ambedkar Circle, Jaipur - 302005, Rajasthan
15	**Local Office (LO)**	**Panji** 6th Floor, EDC House, Atmaram Borkar Road, Panaji - 403007, Goa
16	**Local Office (LO)**	**Raipur** 1st Floor, Investment Building, Phase-I, LIC Campus, Pandri, Raipur - 492004, Chhattisgarh
C		**SRO**
17	**Regional Office (RO)**	**Chennai** 7th Floor, 756-L, Anna Salai, Chennai - 600002, Tamil Nadu
18	**Local Office (LO)**	**Bangalore** 2nd Floor, Jeevan Mangal Building, No.4, Residency Road, Bengaluru - 560025, Karnataka

19	**Local Office (LO)**	**Hyderabad** 1st Floor, Indira Chambers, 8-2 622/5/A/1 Road No. 10, Avenue 4, Banjara Hills, Hyderabad - 500034, Andhra Pradesh
20	**Local Office (LO)**	**Kochi** 6th Floor, Finance Tower, Kaloor, Kochi - 682017, Kerala
21	**Local Office (LO)**	**Vijaywada** K Towers, 2nd floor, D.No.32-6, 14 D, T.N.Rao Street, Visalandhra Road, Praja shakti Nagar,, Vijayawada, , Hyderabad - 520010, Andhra Pradesh
D		**ERO**
22	**Regional Office (RO)**	**Kolkatta** The Regional Director, L&T Chambers, 3rd Floor, 16 Camac Street Kolkata - 700017, West Bengal
23	**Local Office (LO)**	**Bhubaneswar** IDCOL House, Ashok Nagar, Unit - II, Bhubaneswar - 751009, Odisha
24	**Local Office (LO)**	**Guwahati** NEDFI House, 4th Floor G.S. Road, Dispur, Guwahati - 781006, Assam
25	**Local Office (LO)**	**Patna** Udyog Bhawan, 3rd Floor, East Gandhi Maidan, Patna - 800004, Bihar
26	**Local Office (LO)**	**Ranchi** New Collectorate Building, A-Block, Room No. 601 to 604, 6th Floor, Kutchery Road Ranchi - 834001, Jharkhand

iv. Sealed packs shall be opened only in the presence of authorized officials of SEBI. Each case, packing or box shall include inside a copy of the corresponding packing list identifying the contents. While unpacking the goods/products, the Solution Provider shall check physical availability of items as per the packing list.

v. The accessories (utilities, packaged software, etc. including complete set of manuals) as given by the principals' should be delivered with the hardware.

vi. SEBI shall certify the acceptance of the delivered material in accordance with Bill of Materials after checking and inspecting the same.

vii. Delivery of Products shall be deemed to have been made when the contents of the cases, boxes or packages are witnessed together by SEBI and the Solution Provider or their representatives, to be identical to those listed in the packing list included therein, installed and verified the internal components. However, this proof of delivery to the final destination shall in no way absolve or release the Solution Provider from the performance of his warranty obligations under this Agreement.

12.19. Delivery, Installation and Commissioning

i. The Total Solution shall have a complete licensed copy of all the software/hardware/networking/security components.

ii. The Solution Provider shall furnish certified true copies of all back to back license/support agreements entered into by the Solution Provider for providing Total Solution under this Agreement and ensure that the same are valid and in force during the term of this Agreement.

iii. All the goods or products under this Agreement shall be delivered to the final destination specified by SEBI in this regard and all the costs till the time the goods or products are delivered shall be borne by the Solution Provider. The breakup costs of delivery costs like storage, loading, unloading, etc. shall be included in the Agreement Price. All the documents like Invoice, Packing list, Guarantee Certificates, Solution Provider' inspection reports, Insurance certificate, certificate of origin, etc. shall be provided by the Solution Provider to SEBI. The Solution Provider shall also be responsible for the goods/products until their acceptance by SEBI.

iv. The Solution Provider shall be responsible for installation and commissioning of the Systems including cabling and other related activities such as unpacking, uncarting, inspection etc. for which SEBI shall provide the required space. While unpacking and installation, the Solution Provider shall check physical availability of items as per the packing list. Delivery of goods or products shall be deemed to have been made when the contents are installed and components are witnessed together by SEBI and the Solution Provider or their representatives, to be identical to those listed in the packing list included therein. Delivery shall be considered complete only after items are accepted by SEBI. Further, the proof of delivery to the final destination shall in no way absolve/release the Solution Provider from the performance of his warranty obligations under this Agreement.

v. The Solution Provider shall number the systems as indicated by SEBI, at the time of installation and commissioning.

vi. Installation and configuration of the systems at site(s), including unpacking of cartons/boxes, shall be the responsibility of the Solution Provider.

vii. SEBI reserves the right to install third party software/hardware or any other products in the systems as mutually agreed between the parties. In such case, there shall be no change in the warranty terms of the existing system as provided by the Solution Provider.

viii. If SEBI desires to relocate the data centre for SEBI SIT-NET to any other location during the implementation/post implementation, the Solution Provider shall assist in de-installation and re-installation of entire solution. However, this exercise may be on chargeable basis, which shall be reasonable. SEBI reserves the right to shift systems to new locations within the country and the Solution Provider hereby agrees to assist SEBI during such process. The risks and costs of relocation shall be borne by SEBI and in such a case, there shall be no change in the warranty terms. In addition to above, the Solution Provider shall provide necessary assistance and detailed guidelines to SEBI to set up a level 3 data centre at the identified location. SEBI shall bear the responsibility of setting and maintaining the data centre.

ix. The Solution Provider shall not encourage or partake in software piracy in any manner.

12.20. Reference to Expert Committee[9]

All disputes and differences concerning Deliverable and changes of any kind, whatsoever, between the Solution Provider and SEBI, shall be referred to an Expert Committee and the decision of the Expert Committee will be final and binding on the Parties.

The Expert Committee appointed under this clause shall:

i. make a determination based upon the information made available by the Parties;
ii. make a determination having regard to the obligations of the Parties under this Agreement;

---

[9] **"Expert Committee"** means and comprise of independent experts in the field of information technology and finance as appointed by the parties within 2 (two) weeks from Effective Date

iii. notify the Parties in writing of their decision within 10 (ten) Business Days of referral of the dispute;

Expert Committee shall act as experts not as arbitrators and the cost of the Expert Committee's determination shall be borne equally by the Parties;

The Solution Provider shall continue to work under the Agreement during the reference to Expert Committee unless otherwise directed by the Expert Committee or by SEBI in writing, or unless the matter is such that the works cannot possibly be continued until the decision of the Expert Committee, is obtained;

If the dispute is not resolved in the above mentioned resolution phases, then the dispute shall be referred to Arbitration.

12.21. Insurance

a. The Solution Provider shall fully insure each and every goods or products supplied under the total solution against all risks including terrorism, riots and civil commotion, up to the point of installation or up to 60 days from actual delivery date, whichever is earlier, with an insurance company/corporation.
b. The goods supplied under this Agreement shall be fully insured in Indian Rupees naming SEBI as the beneficiary. The Solution Provider shall submit insurance documents along with the delivery of corresponding products to SEBI.
c. In case of any loss or damage occurs, the Solution Provider should be responsible for initiating and pursuing claims and settlement and simultaneously also make arrangements for repair and/or replacement of any damaged item/s.
d. The sum assured shall be 125% of the goods supplied.

12.22. Correspondences

SEBI and the Solution Provider shall nominate a Project Manager each immediately on acceptance of the order, whom shall be the single point of contact for the project at Mumbai. However, for escalation purpose, details of other persons shall also be given. The project manager nominated by the Solution Provider should have prior experience in implementing similar systems in the past.

12.23. Change Management Procedure

i. During the course of implementation, it may be found that certain functionalities have been missed out in the Requirement Gathering Phase. The Solution Provider shall be required to incorporate these functionalities as part of this project. SEBI estimate that effort for such functionalities would be 10% of the total effort estimated for the implementation of the project and the Solution Provider shall provide these services at no additional charge to SEBI. Solution Provider shall be responsible for collation of all such enhancement requests submitted by SEBI. Change Control Requests (CCR) for enhancements shall be generated by SEBI clearly defining the functionality and desired calendar time for the implementation. The Solution Provider shall provide SEBI with a written estimate of the effort necessary for the implementation of the requested enhancements. Upon approval by SEBI, the Solution Provider shall prioritize development and carry out implementation of the enhancements in a controlled and efficient fashion.

ii. Any enhancement effort in addition to the enhancement estimates as mentioned in clause 12.23.i shall be provided on a time and materials basis at the rates agreed by the parties in this regard and also referred to Annexure '__' of this agreement.

iii. The Solution Provider shall provide details of effort estimation methodology followed internally to calculate the effort estimates including the tools and strategy used.

iv. The Solution Provider shall also provide a detailed post-implementation post go-Live change management system including but not limited to:
- Change request procedures
- Software development/customization

v. Documentation which includes design details, test cases executed vulnerability analysis etc. in addition to the user documentation.

vi. In order to ascertain the road map of the proposed solution, the Solution Provider shall submit an assessment of following items but not limited to:
- extent of customization and integration possible
- available and proposed APls
- ability to include new features

12.24. Project Management and Correspondences

i. SEBI shall designate certain positions within Solution Provider's staff as key Solution Provider's personnel and no Solution Provider's personnel shall be designated as a key Solution Provider's personnel unless SEBl's approval is obtained. The Solution Provider shall also, before commencement of each Phase of the Project, identify and designate the key personnel (lead resources) for such Phase.

ii. The Solution Provider shall provide SEBI with the resumes of all personnel it proposes to staff as key Solution Provider's personnel and SEBI shall have the right to approve or reject such personnel in its sole and absolute discretion.

iii. The Solution Provider shall not change any key Solution Provider’s personnel approved by SEBI without the prior written approval of SEBI, which shall not be unreasonably withheld. However, no such approval shall be required in case of death, illness, retirement or resignation of such key Solution Provider personnel.

iv. Prior to replacement of key Solution Provider’s personnel, the Solution Provider should provide to SEBI the resumes of at least two (2) alternate members of its staff who have the same or better experience than the person who is being replaced and any replacement shall happen only once SEBI has approved the replacement personnel and such replacement personnel have had reasonable time to acquaint himself/herself with the functions being discharged by the present incumbent of the key Solution Provider’s personnel position.

v. The Solution Provider's personnel assigned to these positions shall be committed to the SEBI SIT-NET project at least for a period of twenty four (24) months at any given time and the Solution Provider shall also intimate SEBI in advance of any leave proposed to be taken by its key personnel for a minimum period of six (6) months from the date on which completion of the Project.

vi. Each key Solution Provider’s personnel shall execute a Confidentiality and Non-Disclosure Agreement as also an Undertaking inter alia undertaking that they shall not disclose any information acquired while dealing with the Project which is confidential in nature to anybody including their relatives and shall intimate SEBI or the Solution Provider before they or their relatives access the securities market during the implementation period of the Project.

vii. SEBI and the Solution Provider shall each allocate a full time Project Manager who will interact with each other in the implementation of the Project and all other related matters.

viii. SEBl's Project Manager shall be available to the Solution Provider at all reasonable times in matters connected to the assignment and shall be the single point contact in the matters related to the assignment. The Solution Provider's Project Manager shall have the responsibility and the necessary authority to deal with all day-to-day matters under this Agreement on behalf of the Solution Provider.

12.25. Deemed Acceptance

a. In case SEBI (i) does not provide any review comments within the below mentioned period and/or (ii) starts using the Deliverables/ Systems in a live production environment after the below mentioned period, then the Deliverables/Systems shall be deemed to be unconditionally and absolutely accepted by SEBI whether SEBI provides such acceptance certificate to the Solution Provider or not and the Solution Provider shall be entitled to receive the charges due on acceptance.

Table 21: Acceptance Timeline

SI. No	Type of Acceptance	Deemed Acceptance Period
A.	Intermediate acceptance which are not linked to payment terms	30 Business Days
B.	Acceptance at the end of each milestone (where payment would be involved)	45 Business Days
C.	Final Acceptance	60 Business Days

b. If any acceptance test fails at any stage, then it shall be repeated from the beginning, after the Solution Provider rectifies the problem, to comply with the specifications agreed upon by both the Parties and certify that the solution delivered for acceptance test is per the specifications. The deemed acceptance period would in such case recommence from the date of such certification.

12.26. Representation and Warranties

1. The Solution Provider represents and warrants to SEBI as under:

i. that the Solution Provider has the experience and the technical know-how to undertake the Project and provide the Services under this Agreement.

ii. that the Solution Provider has a valid license for the all software which form an integral part of the Total Solution.

iii. The Services and the Systems, Products or any software provided, do not infringe, and shall not infringe or cause the infringement of, the proprietary rights of any third party.

iv. The Service and the System shall utilize current and proven technologies.

v. The Services to be provided hereunder shall be performed with qualified personnel in accordance with the applicable time schedules (or otherwise in a timely manner).

vi. The Services and Systems shall be provided in a good and workman like manner, in accordance with the applicable Technical Specifications and Acceptance Criteria and at least at the same level and with the same degree of accuracy, quality, completeness, responsiveness and cost effectiveness which are consistent with good industry standards.

vii. The Systems, Products or software provided hereunder properly interface with other systems, properly interface with each other, perform together as an integrated system and, as an integrated system, meet the warranties in this Agreement, including but not limited to the meeting of the Technical Specifications.

viii. The Systems provided hereunder shall function as designed and be fit for the purpose for which they have been provided and will be otherwise be free of errors and defects that interrupt systems operations or otherwise negatively impact normal operations or business processes.

ix. During the term of this Agreement, the Services, Systems and any software provided shall not contain or introduce any viruses, bugs or disabling Codes. In the event of any such virus being introduced into SEBI's systems, the Solution Provider shall use its best efforts to minimize the impact of such virus.

2. All the Hardware and Software supplied under this Agreement shall be covered under Warranty for the duration of the 3 years commencing from the date of acceptance of the total solution.

3. The Solution Provider shall undertake to maintain the Total Solution for a minimum period of *4 years* from the date of the expiry of the warranty period, with price break-up for each year. However, SEBI reserves right to enter into AMC for one or more years after Warranty at the finalized price and terms. If the Solution Provider fails to offer AMC for AMC Period (4 years), then the Bid is liable for rejection.

4. SEBI reserves the right to enter into AMC for part or full project/items. During AMC period if a particular product/hardware/software/component/services is discontinued or removed from the AMC contract, SEBI shall not pay the corresponding amount reserved for that components/product/service, etc.

5. SEBI represents and warrants to Solution Provider that all material or information provided by it to the Solution Provider in connection with or for the purposes of this Agreement are either owned by it or under proper license and the use and possession thereof by SEBI in connection with or for the purposes of this Agreement will not Infringe the rights of any third parties.

12.27. Maintenance

The scope of work for the maintenance period shall include:

1. The correction of any defects that may arise from the design or workmanship or from any act or omission of the Solution Provider that may develop under normal use of the supplied Systems. Normal operating environmental conditions shall be specified in the Agreement. On receiving the notification from SEBI, the Solution Provider shall carry out the repair / replace the defective systems as per the SLA's mentioned in the RFP/Purchase order (PO) document. This will be done at no extra cost to SEBI. Failure to remedy the defects within the period specified in this Agreement, may involve remedial action by SEBI at the Solution Provider' risk and expense and without prejudice to any rights that SEBI may have against the Solution Provider under this Agreement.

2. The provision of Emergency Maintenance Support including providing support and remedial services for problems that render the SIT-NET unavailable or unresponsive; resolving any issues and correcting errors within the proposed products /solutions irrespective of the source of such problem; and working closely with SEBI to provide timely problem resolution and contingency planning for the Enterprise SOC and NOC.

3. Corrective maintenance

4. Preventive maintenance

5. Enhancement Services: The Solution Provider shall provide Enhancement Services as per the agreed Change Management Procedure. The Solution Provider shall work with SEBI to package maintenance patches and enhancements into releases based on SEBI's business and technical priorities. Solution Provider may include, in each release, emergency maintenance fixes, and/or critical bug fixes available but not yet implemented. In the case of a release containing maintenance patches and enhancements, only the portion of the release that would otherwise have constituted an Enhancement will be treated as an Enhancement, unless otherwise approved by SEBI.

6. Production Support and continuous improvement support: Solution Provider shall correct all problems with the SIT-NET in all the environments and shall minimize the impact on the total solution, SEBI and the authorized users of the solutions.

7. Fixation of bugs and patches, upgrades, updates, releases, versions of application software and system software, also carry out its implementation

8. The offer must give commitment to provide maintenance at the price quoted for 4 years (mention rates separately for each of the <AMC Period>) from the date of expiry of three-year warranty.

9. Replacement equipment shall be covered under warranty for a three-month period, or the time remaining in the Warranty Period for the item replaced, whichever is greater. The Warranty Period for replacement Software shall be identical to the initial warranty period for the defective Software unless otherwise specified in the agreement/ contract. During the Warranty Period, the Solution Provider will provide at no additional cost to SEBI all Product and documentation updates, releases, upgrades, patches, bug fixes etc. of all products including system software within 15 days of their availability.

10. The AMC payment shall be released quarterly in arrears. SEBI reserves the right to enter into AMC for part or full project/items.

11. As a part of the maintenance agreement/ contract, the Solution Provider shall provide software updates, releases, upgrades, version upgrades, versions etc. of all the Application Software, System Software, Custom Software and any other software included in the Products and also carry out its implementation.

12. SEBI may decide to outsource the maintenance of the systems to a third-party or SEBI may decide to perform the maintenance in-house. In such case, the Solution Provider shall undertake to provide to the persons / agencies, authorized by SEBI for the purpose, requisite maintenance training, technical know-how kits, and expert assistance on terms mutually agreed upon between SEBI and the Solution Provider.

13. The Solution Provider acknowledges that the SIT-NET performs a very important function and that its continued availability of all of the functionality plays an integral role in the effective discharge of roles and functions of SEBI. Hence the Solution Provider agrees that the services provided by the Solution Provider in relation to the technical support and maintenance shall be subject to a service level agreement and appropriate service level commitments. The Solution Provider agrees that in the event that the Solution Provider defaults in meeting such agreed service level commitments, in addition to the other remedies that SEBI has (such as Liquidated Damages), SEBI shall also be entitled to Service level credits as may be agreed to between the Parties.

12.28. Solution Provider's Obligations

i. The following forms illustrative obligations of the Solution Provider. These are not exhaustive.

ii. The Solution Provider shall be solely responsible for the performance and completion of all his obligations.

iii. The Solution Provider shall abide by the job safety, insurance, customs and immigration measures prevalent and laws in force in India, and shall indemnify SEBI and keep SEBI harmless at all times against all demands or responsibilities arising from accidents or loss of life, the cause of which is the Solution Provider's negligence. The Solution Provider shall pay all indemnities arising from such incidents and shall not hold SEBI responsible or obligated.

iv. The Solution Provider shall be responsible for and obligated to conduct all contracted activities with due care and diligence, in accordance with this Agreement and using state-of-the-art methods and economic principles, and exercising all reasonable means to achieve the performance specified in this Agreement.

v. The Solution Provider shall be obliged to give sufficient support to SEBI's staff, work closely with SEBI's staff, act within its own authority, and abide by directives issued by SEBI that are consistent with the terms of the Agreement. The Solution Provider shall be responsible for managing the activities of its personnel and any sub-contracted personnel, and will hold itself responsible for any misdemeanours.

vi. The Solution Provider shall appoint an experienced Representative to manage its performance of the Agreement/ contract within 15 (fifteen) days of signing of the Agreement. The Representative shall be authorized to accept orders and notices on behalf of the Solution Provider, and to generate notices and commit the Solution Provider to specific courses of action within the scope of this Agreement.

vii. The Representative may be replaced only with the prior written consent of SEBI. The Solution Provider shall be solely responsible for the performance of the Agreement to the satisfaction of SEBI.

viii. SEBI shall designate certain positions within the Solution Provider’s staff as key personnel. The Solution Provider’s personnel assigned to these positions shall be committed to the SIT-NET project for a minimum period of 24 months from the date on which they commence work for SEBI under this project. No Solution Provider’s personnel shall be staffed as key Solution Provider’s personnel unless SEBI’s approval is obtained. The Solution Provider must provide SEBI with the resumes of all personnel it proposes to staff as key Solution Provider’s personnel and SEBI shall have the right to approve or reject such personnel in its sole and absolute discretion. The Solution Provider shall not change any key Solution Provider’s personnel approved by SEBI without the prior written approval of SEBI, which shall not be unreasonably withheld. Prior to replacement of key Solution Provider’s personnel, the Solution Provider shall provide the SEBI the resumes of at least 2 (two) alternate members of its staff who have the same or better experience than the person who is being replaced and any replacement shall happen only once SEBI has approved the replacement personnel and such replacement personnel have had reasonable time to acquaint himself/herself with the functions being discharged by the present incumbent of the key Solution Provider’s personnel position.

ix. The Solution Provider shall always send trained and experienced engineers to provide services at required locations of SEBI. Their name, contact address and phone nos. shall be advised in writing to SEBI.

x. Whenever any designated personnel of the Solution Provider is leaving his job, the Solution Provider shall immediately inform the same on receipt to give prior information about this to SEBI.

xi. The Solution Provider's engineer(s) shall always work on SEBI networks & devices from SEBI premises and shall never enter into SEBI network from any other public or private network under any circumstance.

xii. The Solution Provider’s engineer(s) shall not change the password of network, security devices / applications software / tools without the knowledge of SEBI's IT Team. In case they are aware about any password(s), they shall not share it with anyone other than SEBI’s team without prior written approval from SEBI’s Team.

xiii. If necessary, SEBI may escalate the call to higher authorities of the Solution Provider. In that case, the Solution Provider shall put their maximum efforts and deploy their best resources to resolve the calls at the earliest possible time frame at all locations and ensure appropriate uptime.

xiv. The Solution Provider shall be responsible for any or all act of its employees that may result in security breach in respect of SEBI network.

xv. The Solution Provider shall assign personnel of appropriate qualifications and experience to perform the services in order to fulfil its obligations.

xvi. The Solution Provider shall designate one of its personnel as the Project Manager, to interact with the Designated Customer Support Contact from SEBI for the purposes of getting approvals, progress report, discussing and resolving issues, arranging meetings, etc.

xvii. The Solution Provider shall exercise requisite control and supervision over its personnel in the course of rendering the services and make best efforts to ensure that the services are rendered in a continuous and uninterrupted manner.

xviii. The Solution Provider shall always respect the confidentiality of all information given to it by SEBI and shall not divulge such information to any third party or other units without the prior written consent of SEBI.

xix. The Solution Provider shall promptly install/implement the corrected licensed software and/or maintenance releases provided at the Designated Location(s) of SEBI at no additional cost or fees or expenses.

xx. The Solution Provider shall undertake regular preventive maintenance of the licensed software.

xxi. All bug fixations / modifications / enhancements relating to the licensed software shall be done by the Solution Provider in a time bound manner as per the SLA. The Solution Provider shall adopt a common, smooth, timely and effective and satisfactory bug/enhancement handling mechanism. The Solution Provider agrees that the errors resulting from the licensed software shall not be attributed to alleged misuse, improper use, alteration or damage by users. The Solution Provider shall compensate SEBI such financial loss suffered by SEBI if the Solution Provider fails to fix bugs, provide the modifications / enhancements / customization as required by SEBI as per the terms and conditions of this Agreement and to meet the services level agreements as will be entered into by the Solution Provider with SEBI.

xxii. The Solution Provider is obliged to work closely with SEBI's staff, act within its own authority and abide by directives / instructions issued by SEBI from time to time. The Solution Provider will abide by the job safety measures prevalent in India and will free / indemnify Purchaser from all demands or responsibilities arising from accidents or loss of life, the cause of which is the Solution Provider's negligence. The Solution Provider shall pay all indemnities arising there from and shall not hold SEBI responsible or obligated.

xxiii. The Solution Provider shall be required to develop, maintain and manage the proposed services to enable SEBI to meet its requirements. It shall be the Solution Provider's responsibility to ensure compliance to the requirements of the continued operation of the intended services in accordance with and in strict adherence to the terms of this Bid, the RFP and this Agreement.

xxiv. In addition to the aforementioned, the Solution Provider shall ensure that the Solution Provider's Team is competent, professional and possesses the requisite qualifications and experience appropriate to the task they are required to perform under this Agreement. The Solution Provider shall ensure that the Services are performed through the best efforts of the Solution Provider's Team, in accordance with the terms hereof and as per Acceptance Criteria. Nothing in this Agreement shall be considered to relieve the Solution Provider from its liabilities or obligations under this Agreement to provide the Services in accordance with the SEBI's directions and requirements and as stated in this Agreement and the Bid to the extent accepted by the SEBI and the Solution Provider shall be liable for any non-performance, non-compliance, breach or other loss and damage resulting either directly or indirectly by or on account of its Team.

xxv. All personnel so employed/engaged by the Solution Provider shall all times be the employees of the Solution Provider under all statutes and in case any dispute arises between such personnel and the Solution Provider, it shall be resolved and settled between them. The Solution Provider agrees and undertakes that in no way the Solution Provider shall involve SEBI in any of their grievances and/or disputes. The Solution Provider undertakes to indemnify SEBI against any and all claims, proceedings, actions, damages, losses, costs and expenses arising out of a) such grievances or disputes b) noncompliance of applicable law c) non-payment / delays in payment of dues of its employees d) settlement / payments of any claim or penalty or dues pertaining to employees of the Solution Provider d) cost of litigation, proceeding including fees of legal professionals engaged by SEBI for defending or responding or pursuing such litigation / proceedings. The Solution Provider shall maintain all books and records as are required to be maintained under the applicable rules, regulations and laws including muster roll, wage register, leave register etc. and the Solution Provider shall be solely and personally responsible and liable for the breach of any or all of the statutory obligations in respect of all its employees etc. engaged under this Agreement and SEBI shall in no way be held responsible for any breach committed by the Solution Provider in this regard. During the terms of this Agreement as well as after expiry / termination of this Agreement, SEBI shall not have any privity of contract with designated employs of the Solution Provider.

xxvi. SEBI shall not be held liable or responsible for any claim (monetary or otherwise), damage (of any kind) or liability suffered by the Solution Provider and/or its employees, employed / engaged for providing services under this Agreement. The Solution Provider undertakes that no claim / dispute shall be raised against SEBI by contractors or employees engaged by the Solution Provider.

xxvii. The Solution Provider shall supply to the SEBI, at least 10 (ten) days prior to the effective date of commencement of works/services or kick-off meeting whichever is earlier, an organization chart showing the proposed organization/manpower to be established by the Solution Provider for execution of the work/facilities/services including the identities and Curriculum-Vitae of the key personnel to be deployed. The Solution Provider shall inform SEBI in writing in advance, of any revision or alteration of such organization charts.

xxviii. The Solution Provider shall provide necessary supervision during the site preparation and installation of the equipment at the Data Centre and as long thereafter as SEBI may consider necessary for the proper fulfillment of the Solution Provider’s obligations under this Agreement. The Solution Provider or his competent and authorized representative(s) shall be constantly present at the whole time for supervision. The Solution Provider shall authorize the Supervisor or his representative to receive directions and instructions (if any) from SEBI’s Representative.

xxix. The Solution Provider shall be responsible for the deployment, transportation, accommodation and other requirements of all its employees required for the execution of the work and for all costs/charges in connection thereof or incidental thereto.

xxx. The Solution Provider shall provide and deploy, on the Site for carrying out the work, only those manpower resources who are skilled and experienced in their respective trades and who are competent to execute or manage/supervise the work in a proper and timely manner.

xxxi. SEBI’s Representative may at any time object to and require the Solution Provider to remove forthwith from the site a supervisor or any other authorized representative or employee of the Solution Provider or any person(s) deployed by Solution Provider, if, in the opinion of SEBI’s Representative the person in question has misconducted himself or his deployment is otherwise considered undesirable by SEBI’s Representative. The Solution Provider shall forthwith remove and shall not again deploy the person in question at the work site without the prior written consent of SEBI’s Representative.

xxxii. SEBI’s Representative may at any time direct the Solution Provider to remove from the work / Site the Solution Provider’s supervisor or any other authorized representative including any employee of the Solution Provider or any person(s) deployed by the Solution Provider for professional incompetence or negligence or for being deployed for work for which he is not suited. The Solution Provider shall take necessary steps to remove that person from deployment on the work, which the Solution Provider shall then forthwith do and shall not again deploy any person so objected to on the work or on the sort of work in question (as the case may be) without the written consent of SEBI’s Representative.

xxxiii. The Solution Provider shall maintain backup personnel and shall promptly provide replacement of every person removed, pursuant to this section, with an equally competent substitute from the pool of backup personnel.

xxxiv. In case of change in its team composition owing to attrition, the Solution Provider shall ensure a reasonable amount of time-overlap in activities to ensure proper knowledge transfer and handover/takeover of documents and other relevant materials between the outgoing and the new member. The exiting team member should be replaced with an equally competent substitute from the pool of backup personnel. The Solution Provider shall ensure that the project or services should not be adversely affected due to any change in team deployed / engaged to provide Services under this Agreement.

xxxv. The Solution Provider shall comply with the provision of all laws including Information Technology Act (as amended), labour laws, rules, regulations and notifications issued there under from time to time. The Solution Provider shall comply with all norms relating to data protection including any law or rules or regulations that may be in force during the term of this Agreement. All safety and labour laws enforced by statutory agencies and by SEBI shall be applicable in the performance of this Agreement and Solution Provider shall abide by these laws.

xxxvi. The Solution Provider shall promptly but not later than two days, report to the SEBI any evidence, which may indicate or is likely to lead to an abnormal or dangerous situation and shall take all necessary emergency control steps to avoid such abnormal situations.

xxxvii. The Solution Provider shall also adhere to all security requirement/regulations of the SEBI during the execution of the work.

xxxviii. The Solution Provider and its employees shall ensure to obtain permissions for bringing or using any electrical equipment, portable devices etc. from SEBI.

xxxix. The Solution Provider and its employees shall always adhere to internal security and safety policies of SEBI.

xl. The Solution Provider shall put all efforts to ensure that no Computer Virus is introduced onto SEBI's or any user's computer equipment or systems by any act, omission or negligence of the Solution Provider or its employees. The User shall mean any entity using services, software, systems etc. provided by SEBI or licensed to SEBI.

Access to the SEBI Data Centre should be strictly restricted in the following manner:

a) No access to any person except one explicitly authorized by SEBI shall be allowed entry. Even if granted, access shall be restricted to the pertaining equipment of SEBI only and access to any other equipment must be strictly precluded by necessary means, locks, video surveillance, etc.

b) No access to any person (even if authorized by SEBI) shall be allowed without being unaccompanied by a security staff at all times during his/her presence in the Data Centre area and subject to recorded video surveillance.

c) No access to any employee of the Solution Provider, except the essential staff who have genuine work- related need, shall be given. All such access shall be logged in a loss-free manner for permanent record with unique biometric identification of the employee to avoid misrepresentations or mistakes.

12.29. Agreement/ contract Amendments

Any change made in any clause or clauses of this Agreement which shall modify the purview of this Agreement within the validity and currency of this Agreement shall be deemed as an Amendment. Such an Amendment can and shall be made and be deemed legal only when the Parties to this Agreement provide their written consent about the Amendment, subsequent to which the Amendment shall be duly signed by the Parties and shall be construed as a part of this Agreement. The details of the procedure for Amendment may also be specified in the Amendment.

12.30. Applicable Law and Jurisdiction

The law governing this Agreement shall be the laws of India and the Courts in Mumbai shall have exclusive jurisdiction to adjudicate any dispute(s) that may arise in connection or in relation to this Agreement including its interpretation thereof, irrespective of the place of the cause of action and rights and liabilities of the Parties hereto.

12.31. Governing Language

All correspondences and other documents pertaining to this Agreement shall be in English only.

12.32. Limitation of Liability

i. The Solution Provider shall be excused and not be liable or responsible for any delay or failure to perform the Services or failure of the Services or a Deliverable under this Agreement to the extent that such delay or failure has arisen as a result of any delay or failure by SEBI or its employees or agents or third party service providers to perform any of its duties and obligations as set out in this Agreement. In the event that the Solution Provider is delayed ·or prevented from performing its obligations due to such failure or delay on the part of or on behalf of SEBI, then the Solution Provider shall be allowed an additional period of time to perform its obligations and unless otherwise agreed the additional period shall be equal to the amount of time for which the Solution Provider is delayed or prevented from performing its obligations due to such failure or delay on the part of or on behalf of SEBI. Such failures or delays shall be brought to the notice of SEBI, immediately within 2 (two) days of occurrence such failures or delays and subject to mutual agreement with SEBI, the Solution Provider shall take such actions as may be necessary to correct or remedy the failures or delays and maintain record of all such incidents.

ii. Notwithstanding anything contained in this Agreement the total cumulative liability of either party arising from or relating to this Contract shall not exceed the total amount paid to the Solution Provider by SEBI under this Agreement (excluding the taxes, reimbursements etc.) during the **12 months** prior to the claim date that gives rise to such liability (as of the date the liability arose); provided, however, that this limitation shall not apply to any liability for damages arising from (a) willful misconduct or (b) indemnification against third party claims for infringement.

iii. Neither party will be liable for any indirect or remote damages under the Agreement.

12.33. Extension of Bank Guarantees

The Solution Provider shall be responsible for extending the validity date and claim period of all the bank guarantees as and when it is due on account of incompletion of work under guarantees. SEBI shall invoke the guarantee before expiry of validity if work is not completed and the guarantee is not extended, accordingly.

12.34. Stamp Duty

The stamp duty and any other incidental charges payable on this Agreement shall be borne and paid by the Solution Provider.

12.35. Order of Precedence

It is understood by the Parties that certain technical statements made in other documents may be additive and not considered conflicting or ambiguous. The order of Precedence shall be as follows:

(i) The terms and conditions of this Agreement and the appendices attached to this Agreement;

(ii) SEBl's Request For Proposal dated December 24, 2020 Clarifications to the RFP issued by SEBl; Other Communications carried out through paper, email and, written submissions in meetings held for the purpose of this project;

(iii) Solution Provider's Proposal dated *<Date of RFP>*; Solution provider's addendum

For the avoidance of doubt, the most recent document takes precedence in the event of ambiguity or conflict between the Contract Documents.

12.36. Exit Management / Transition Support

1. During the acceptance test, the Solution Provider shall provide at least two expert personnel at the site on a full time basis, in addition to such other personnel as may be deployed at the site by the Solution Provider for performance of this Agreement. These personnel shall be responsible for all transition supports, necessary to complete the acceptance test on the Systems. The details of the transition support shall be specified in the agreement/ contract
2. In the event that the SEBI decides to award the AMC (4th, 5th, 6th, 7th year) to any third party, the Solution Provider shall provide detailed termination assistance services to SEBI and/or a successor Solution Provider on termination/expiry of the AMC which shall enable SEBI/the successor Solution Provider to assume AMC responsibilities without any deterioration in the service levels.

3. The Solution Provider shall provide a comprehensive exit management/transition out plan to ensure smooth transfer of the services so as to continue to meet SEBI's business requirements in a way that minimizes unplanned business interruptions.
4. The Solution Provider shall include a project plan ("Transition Project Plan") indicating the tasks, timeframes, resources, and responsibilities associated with the transition activities.
5. The Solution Provider shall ensure that all the documentation required for smooth transition including configuration documents are kept up to date and is made available to SEBI at regular intervals as well as during the exit management process.

12.37. Sole Point of Contact:

Irrespective of whether or not the Solution Provider is the sole provider of the services and the systems that comprise the SEBI SIT-NET, the Solution Provider / lead Solution Provider in case of consortium shall be liable to SEBI for the provision of the SIT-NET as contracted between SEBI and itself. The Solution Provider shall not be allowed to rely on failure by a third party (whether a consortium member or a subcontractor) to provide any hardware, software or services to excuse itself from a delay or a failure to discharge its obligations under this agreement/ contract.

12.38. Reporting Progress of the Project

The Successful Solution Provider shall monitor progress of all the activities specified in the program of works and submit free of cost weekly progress report about various aspect of the works/Services to the SEBI including hindrance if any. The Successful Solution Provider shall provide inventory details at the end of each month as per SEBI format.

12.39. Adherence to safety procedures, rules, regulations and restriction

1. The Solution Provider shall comply with the provision of all laws including labour and industrial laws, rules, regulations and notifications issued there under from time to time. All safety and labour and industrial laws enforced by statutory agencies and by SEBI shall be applicable in the performance of this Agreement and the Solution Provider shall abide by these laws. The Solution Provider shall indemnify and keep indemnified and hold harmless the SEBI for any loss, damage, claims, costs, charges, expenses, etc. arising out of and/or suffered on account of actions, litigations, proceedings, suits, arising out of breach of the above laws.
2. The Solution Provider shall take all measures necessary or proper to protect the personnel, work and facilities and shall observe all reasonable safety rules and instructions.
3. The Solution Provider shall also adhere to all security requirement/regulations of the SEBI during the execution of the work.

12.40. Termination

a. It is agreed, without prejudice to any other remedy available in case of default on the part of either Party in the performance of this Agreement or in the discharge of any contractual obligations arising out of this Agreement, that either Party may terminate this Agreement if the other Party commits substantial breach of its obligations including but not limited to payment and such breach is not corrected within 30 (thirty) days from the date of receipt, by the defaulting Party, of a written notice of intended termination !rom the other Party, provided however that this period may be extended for an additional period of 30 (thirty) days, if the defaulting Party, has taken necessary steps to cure such breach under advice to the other Party.

b. SEBI may at any time terminate this Agreement if the Solution Provider:

   i. has winding-up or insolvency proceedings commenced against it which are not withdrawn within 14 (fourteen) days of such commencement;
   ii. is placed in voluntary liquidation or has a receiver, receiver and manager or other administrator nominated by a creditor or creditors appointed in respect of its assets;
   iii. enters into or proposes to enter into any scheme of arrangement or any composition for the benefit of its creditors, save for the purpose of solvent reconstruction;
   iv. becomes subject to any event analogous to, or enters into any arrangement analogous to, any of those events or arrangements referred to in paragraphs above;
   v. has change in its ownership or control so as to materially impede its ability to discharge its obligations under this agreement; or,
   vi. is not able to perform any or all of its contractual obligations pursuant to Force Majeure.

c. In the event of this Agreement being terminated, SEBI shall be liable to make complete payments of the amount due under this Agreement up to the effective date of termination for which services (including parts thereof) have been rendered by the Solution Provider and such committed costs for software licenses and hardware that Solution Provider has incurred for provision of services to SEBI under this Agreement as per Payment for deliverables clause. In case SEBI suspends or keeps on hold the Project for any reason whatsoever, SEBI shall be liable to make payments for the services rendered by the Solution Provider till the effective date of such suspension or withholding of project.

d. Forthwith on the expiry or earlier termination of this Agreement, each Party shall, return to the other party all documents and materials, belonging to the other party with regard to this Agreement, or shall at the option of the· disclosing party destroy under written certification all documents or materials in connection with this Agreement in a manner under the written certification of the key personnel of

SEBI as well as Solution provider that its subsequent retrieval by whatever means is rendered impossible.

12.41. Conflict Of Interest

The Solution Provider shall disclose to the SEBI in writing, all actual and potential conflicts of interest that exist, arise or may arise (either for the Solution Provider or the Solution Provider's team) in the course of performing the Services as soon as practical after it becomes aware of that conflict.

12.42. Entire Agreement

This Agreement sets forth the entire understanding of the parties with respect to the subject matter hereof and thereof. This Agreement supersedes all prior or simultaneous representations, discussions, negotiations, letters, proposals, agreements and understandings between the parties hereto with respect to the subject matter hereof, whether written or oral. Each Party acknowledges that it has not relied on or been induced to enter into this Agreement by a representation or warranty other than those expressly set out in this Agreement. To the extent permitted by applicable law, a Party is not liable to another Party in contract or tort or in any other way for a representation or warranty that is not set out in this Agreement.

12.43. Audits

SEBI can, at any time, conduct any third party inspections / audits during the tenure of this Agreement. The Solution Provider must make all necessary changes (for the in scope devices /applications) as mentioned by the results of these audits. SEBI shall incur the cost of appointment of a third party for audit. The Solution Provider shall ensure that the findings of the audit are successfully closed by the bidder within a mutually agreed timeline.

1. Appendix X: Service Level Agreement

THIS AGREEMENT is made on this the _____ day of _____ 20__ at ___________, India.

BETWEEN

SECURITIES AND EXCHANGE BOARD OF INDIA, established under the Securities and Exchange Board of India Act, 1992 having its office at SEBI Bhavan, Plot No. C4-A, “G Block”, Bandra Kurla Complex, Bandra (E), Mumbai 400 051, India, hereinafter referred to as “**SEBI**” (which expression shall, unless it be repugnant to the context or meaning thereof, be deemed to mean and include its successors) of the First Part.

AND

____________, a Company incorporated under the Companies Act, 1956, having its registered office at ____________ (hereinafter referred to as ‘the Solution Partner/SI’ which expression shall, unless the context otherwise requires, include its permitted successors and assigns).

Each of the parties mentioned above are collectively referred to as the ‘***Parties***’ and individually as a ‘***Party***’.

WHEREAS:

1. SEBI is desirous to implement the project of------------------------.

2. SEBI and Solution Partner have entered into a Master Services Agreement dated <date> (the “***MSA***”).

NOW THEREFORE, in consideration of the mutual covenants, promises, assurances, representations and provisions set forth herein, the Parties hereto agree as follows:

1. DEFINITIONS AND INTERPRETATION

1.1 Definitions

Terms and expressions used in this Agreement (including the Introduction) shall have the meanings set out in Annexure A.

1.2 Interpretation

In this Agreement, unless otherwise specified:

(a) references to Clauses, Sub-Clauses, Paragraphs and Schedules are to clauses, sub clauses, paragraphs of and schedules to this Agreement;

(b) use of any gender includes the other genders;

(c) references to a ‘**company**’ shall be construed so as to include any company, corporation or other body corporate, wherever and however incorporated or established;

(d) references to a ‘**person**’ shall be construed so as to include any individual, firm company, government, state or agency of a state, local or municipal authority or government body or any joint venture, association or partnership (whether or not having separate legal personality);

(e) a reference to any statute or statutory provision shall be construed as a reference to the same as it may have been, or may from time to time be, amended, modified or reenacted;

(f) any reference to a ‘**day**’ (including within the phrase ‘business day’) shall mean a period of 24 hours running from midnight to midnight;

(g) references to a **‘business day’** shall be construed as a reference to a day on which SEBI conducts regular business;

(h) references to times are to Indian Standard Time;

(i) a reference to any other document referred to in this Agreement is a reference to that other document as amended, varied, novated or supplemented at any time; and

(j) all headings and titles are inserted for convenience only. They are to be ignored in the interpretation of this Agreement.

1.3 Measurements and Arithmetic Conventions

All measurements and calculations shall be in the metric system and calculations done to 2 (two) decimal places, with the third digit of 5 (five) or above being rounded up and below 5 (five) being rounded down except in money calculations where such amounts shall be rounded off to the nearest INR.

1.4 Ambiguities within Agreement

In case of ambiguities or discrepancies within this Agreement, the following principles shall apply:

(a) as between two Clauses of this Agreement, the provisions of a specific Clause relevant to the issue under consideration shall prevail over those in a general Clause;

(b) as between the provisions of this Agreement and the Schedules, the Agreement shall prevail, save and except as expressly provided otherwise in the Agreement or the Schedules; and

(c) as between any value written in numerals and that in words, the value in words shall prevail.

1.5 Priority of agreements

The Parties hereby expressly agree that for the purpose of giving full and proper effect to this Agreement, the MSA and this Agreement shall be read together and construed harmoniously. In the event of any conflict between the MSA and this Agreement, the provisions contained in the MSA shall prevail over this Agreement.

2. STRUCTURE

This SLA shall operate as a legally binding services agreement specifying terms which apply to the Parties in relation to the provision of the Services by the Solution Partner to SEBI and its nominated agencies under this Agreement and the MSA.

3. OBJECTIVES OF THIS SLA

The Solution Partner shall be required to ensure that the Service Levels which shall ensure the following but not limited to:

(a) Improving the efficiency, accuracy and service delivery of operations for SEBI.
(b) Leveraging the benefits in new system in order to:
    (i) Guarantees levels of reliability, availability and responsiveness to systems and applications
    (ii) Provide inbuilt mechanism of security, privacy and quality control for IT Infrastructure.
    (iii) Generate meaningful MIS/Reports from the system.

To meet the aforementioned objectives the Solution Partner will provide the Service Levels in accordance with the performance metrics as set out in detail in this Agreement. Further this Agreement shall govern the provision of the contracted services of the Solution Partner to SEBI from the Go-Live Date.

4. SCOPE OF SLA

This Agreement has been executed in relation to the outsourcing portion of the Project between the Parties. The detailed Service Levels have been set out in Annexure B to this Agreement.

This Agreement shall ensure the following:

(a) Establishment of mutual responsibilities and accountability of the Parties;
(b) Definition each Party’s expectations in terms of services provided;
(c) Establishment of the relevant performance measurement criteria;
(d) Definition of the availability expectations;
(e) Definition of the escalation process;
(f) Establishment of trouble reporting single point of contact; and
(g) Establishment of the framework for SLA change management

The following parties are obligated to follow the procedures as specified by this Agreement:

(a) SEBI
(b) Solution Partner

5. AGREEMENT OWNERS

The following personnel shall be notified to discuss the Agreement and take into consideration any proposed SLA change requests:

	Title	Telephone	Email
SEBI	Authorized Representative		
Solution Partner			

6. CONTACT LIST

In the event that there is any change in the listed contacts, the same shall be communicated and updated prior to such change occurring. The Single Point of Contact ("***POC***") for the Solution Partner shall be ________________ and will be available 24X7.

	Title	Location	Telephone
SEBI	Authorized Representative		
Solution Partner			

7. PRINCIPAL CONTACTS

SEBI and the Solution Partner will nominate a senior staff member to be the principal contact regarding operation of this Agreement. At the date of signing of this Agreement, the nominated principal contacts are:

SEBI principal contact: __________________________

Solution Partner principal contact: __________________________

8. COMMENCEMENT AND DURATION OF THIS AGREEMENT

Agreement shall commence on the date of Go-Live (hereinafter the "***SLA Effective Date***") and shall, unless terminated earlier in accordance with its terms or unless otherwise agreed by the Parties, expire on the date on which this Agreement expires or terminates, which shall be a specific period starting from the *Go-Live Date.*

9. TERMS OF PAYMENT AND LIQUIDATED DAMAGES

(a) In consideration of the Services and subject to the provisions of the MSA and this Agreement, SEBI shall pay the amounts in accordance with the Terms of Payment Schedule of the MSA.

(b) For the avoidance of doubt, it is expressly clarified that SEBI and/or its nominated agencies may also calculate a financial sum and debit the same against the terms of payment as defined in the Terms of Payment Schedule of the MSA as a result of the failure of the Solution Partner to meet the Service Levels as set out in Annexure B of this Agreement, such sum being determined in accordance with the terms of the Service as set out in Annexure B of this Agreement.

10. UPDATING OF THIS AGREEMENT

(a) The Parties anticipate that this Agreement shall need to be re-evaluated and modified to account for changes in work environment and technology from time to time. Hence, they hereby agree to revise the terms of the Agreement on an annual basis.

(b) The Parties hereby agree upon the following procedure for revising this Agreement:

(i) Any and all changes to this Agreement will be initiated in writing between SEBI and the Solution Partner. The service levels in this Agreement shall be considered to be standard for SEBI and shall only be modified if both Parties agree to an appended set of terms and conditions;

(ii) Only SEBI or the Solution Partner may initiate a revision to this Agreement;

(iii) A notice of the proposed revision (“***SLA Change Request***”) shall be served to SEBI or the Solution Partner as the case may be;

(iv) The SLA Change request would be deemed to be denied in case it is not approved within a period of 30 days;

(v) In the event that SEBI/Solution Partner approves of the suggested change the change shall be communicated to all the Parties and the SLA Change request would be appended to the Agreement;

(vi) SEBI shall update and republish the text of Agreement annually to include all the SLA Change Requests that have been appended to the Agreement during the course of the year. Such republished Agreement shall be circulated to all the Parties within 15 days of such change taking place.

11. DOCUMENT HISTORY

All revisions made to this Agreement shall be listed in chronological order as per the format set out below and a copy of the same shall be provided to the Parties:

Version	Date	Description of changes

12. SCOPE OF SERVICES

(a) The Solution Partner shall ensure that Services are available at various locations as per the requirements of the project;

(b) The Solution Partner shall provide support services for addressing problems related to the provision of services of the selected bidder through the POC. Such POC shall be available over telephone on ___________ number 24 hours a day, 7 days a week

(c) The Solution Partner guarantees that it shall achieve the Service Levels for the Project;

(d) The Solution Partner shall be liable to liquidated damages in case of failure to comply with the Service Levels. However any delay not attributable to the Solution

Partner shall not be taken into account while computing adherence to the Service Levels.

13. PERFORMANCE REVIEW

The POC's of both SEBI and the Solution Partner shall meet on a quarterly basis to discuss priorities, service levels and system performance. Additional meetings may be held at the request of either the Solution Partner or SEBI. The agenda for these meetings shall be as follows:

(a) Service performance;
(b) Review of specific problems/exceptions and priorities; and
(c) Review of the operation of this Agreement and determine corrective action to overcome deficiencies.

IN WITNESS WHEREOF THE PARTIES HAVE EXECUTED AND DELIVERED THIS AGREEMENT ASOF THE DATE FIRST ABOVE WRITTEN.

SIGNED, SEALED AND DELIVERED	SIGNED, SEALED AND DELIVERED
For and on behalf of the Implementation Agency by:	For and on behalf of SEBI by:
(Signature)	(Signature)
(Name)	(Name)
(Designation)	(Designation)
(Address)	(Address)
(Fax No.)	(Fax No.)

In the presence of:
1.
2.

Annexure A – DEFINITIONS (SLA)

Agreement	means this Service Level agreement together with all Articles, Annexures, Schedules and the contents and specifications of the RFP;
Applicable Law(s)	means any statute, law, ordinance, notification, rule, regulation, judgment, order, decree, bye-law, approval, directive, guideline, policy, requirement or other governmental restriction or any similar form of decision of, or determination by, or any interpretation or administration of SEBI as may be in effect on the date of the execution of this Agreement and during the subsistence thereof, applicable to the Project;
Business Hours	shall mean the working time for Purchaser users which is <*time to time*> daily. It is desired that IT maintenance, other batch processes (like backup) etc. should be planned so that such back-end activities have minimum effect on the performance;
Effective Date	shall have the same meaning ascribed to it in Clause 8;
MSA	shall have the same meaning ascribed to it in Recital 2;
Parties	means SEBI and Solution Partner for the purposes of this Agreement; “Party” shall be interpreted accordingly;
POC	shall have the same meaning ascribed to it in Clause 6
Project	shall have the same meaning ascribed to it in Recital 1;
SLA Change Request	shall have the same meaning ascribed to it in Clause 11 (b) (iii);
Service Level	means the level of service and other performance criteria which will apply to the Services as set out in the SLA parameters effective during the Term of this Agreement;
Term or Agreement Period	Means the duration of this Agreement.

Annexure B – SERVICE LEVEL AGREEMENT

Definition:

SLA Credit represents amount (in percentage) to be deducted from the bidder.

SLA Credit will be computed on a monthly basis based on the below table. 3 monthly SLA Credit will be averaged at the time of quarterly payment (QP) computation.

SLA will be calculated month wise per occurrence basis.

Table 22: SLA calculation

Sr. No.	**Parameter**	**Baseline**		**Low Performance**		**Adverse Performance**		**Breach**	
			SLA Credit (in % of QP)		**SLA Credit (in % of QP)**		**SLA Credit (in % of QP)**		**SLA Credit (in % of QP)**
1	**Network Devices**								
	Uptime Availability - Uptime availability of system including all associated services	>=99.99%	0	>=98.99% to 99.99%	3	>=97.99% to 98.99%	7	<97.99%	10
	(Tolerance of)			1%		2%		3%	
2	**Solution for NAC**								
	Uptime Availability -	>=99.99%	0	>=98.99% to 99.99%	3	>=97.99% to 98.99%	7	<97.99%	10
	(Tolerance of)			1%		2%		3%	
3	**Solution for Virtual Private Network (VPN)**								
	Uptime Availability -	>=99.99%	0	>=98.99% to 99.99%	3	>=97.99% to 98.99%	7	<97.99%	10

	(Tolerance of)			1%		2%		3%	
4	**Solution for Network Security**								
	Uptime Availability -	>=99.99%	0	>=98.99% to 99.99%	3	>=97.99% to 98.99%	7	<97.99%	10
	(Tolerance of)			1%		2%		3%	
5	**Solution for AD/DNS/DHCP**								
	Uptime Availability -	>=99.99%	0	>=98.99% to 99.99%	3	>=97.99% to 98.99%	7	<97.99%	10
	(Tolerance of)			1%		2%		3%	
6	**Solution for IP telephony**								
	Uptime Availability Uptime availability of system including all associated services	>=99.95%	0	>=98.95% to 99.95%	3	>=97.95% to 98.95%	7	<97.95%	10
	(Tolerance of)			1%		2%		3%	
7	**Solution for Video Conferencing**								
	Uptime availability of system including all associated services	>=99.95%	0	>=98.95% to 99.95%	3	>=97.95% to 98.95%	7	<97.95%	10
	(Tolerance of)			1%		2%		3%	
8	**Solution for SDN**								
	Uptime availability of system	>=99.95%	0	>=98.95% to	3	>=97.95% to 98.95%	7	<97.95%	10

	including all associated services			99.95%					
	(Tolerance of)			1%		2%		3%	
9	**Backup Activity**								
	No. of missed events[10]	1 day	0	2 days	3	4 days	7	6 days	10
	(Tolerance of)			1%		2%		3%	
10	**Wi-Fi**								
	Uptime availability of system including all associated services	>=99.95%	0	>=98.95% to 99.95%	3	>=97.95% to 98.95%	7	<97.95%	10
	(Tolerance of)			1%		2%		3%	
11	**Patch Management**								
	Uptime availability of system including all associated services	>=99.95%	0	>=98.95% to 99.95%	3	>=97.95% to 98.95%	7	<97.95%	10
	(Tolerance of)			1%		2%		3%	
Network Services – Performance Metrics									
10	IP telephony / etc. etc. - Login	Within 30 seconds	0			Within 1 minute	5	Within 2 min	10
11	Wi-Fi – on boarding of new device	Within 2 min	0			>2 min to <5 min	5	>10 min	10
	Wi-Fi connection – subsequent connection	Within 15 seconds	0			Within 1 minute	5	Within 5 min	10

---

[10] If backup is not taken as per schedule i.g. daily backup missed. Example: **Case 1:** Backup scheduled on June 01, 2021. Actual back taken on June 02, 2021 then one day will be counted for SLA. **Case 2:** Backup scheduled on June 01, 2021. Actual back taken on June 03, 2021 then two days will be counted for SLA.

12	NAC– on boarding of new device	Within 1 min	0			>1 min to <2 min	5	>2 min	10
	NAC- connection – subsequent connection	Within 15 seconds	0			Within 1 minute	5	Within 2 min	10
13	VPN - on boarding of new device	Within 5 min	0			>5 min to <10 min	5	>10 min	10
	VPN – subsequent connection	Within 30 seconds	0			Within 1 minute	5	Within 5 min	10
14	Video Conferencing	Within 1 min	0	>1 min to <2 min	3	>2 min to <5 min	7	>10 min	10
15	AD/DNS/DHCP – dynamic allocation of IP	Within 30 seconds	0			>30 seconds to <2 min	5	>2 min	10
16	SDN – change in status of device	Within 1 min	0	>1 min to <2 min	3	>2 min to <5 min	7	>10 min	10
Service levels for Disaster Recovery									
17	Adherence to RTO	100%	0	>=95 % to 100 %	3	>=85% to <95%	7	<85%	10
18	Adherence to RPO	100%	0	>=95 % to 100 %	3	>=85% to <95%	7	<85%	10
Incident and Helpdesk									
19	Support Staff Availability	100%	0			>=98% to <100%	5	<98%	10
20	L1 Support Resolution time Resolution time by L1 support at help desk where incident is logged. Activities under L1 support to be agreed with SEBI.	<= 4 office hours	0			> 4 hours and <= 8 office hours	5	> 8 working hours	10

21	L2 Support Resolution time Resolution time by L2 support at help desk where incident is logged. Activities under L2 support to be agreed with NA.	<= 24 hours	0			> 24 hours and <= 2 days	5	> 2 days	10

2. Appendix XI - Undertaking of Confidentiality and Non-Disclosure

<Applicable only where SEBI needs to provide data to Bidders for Proof of Concept>

This has reference to the data to be provided by Securities Exchange Board of India to <Organization Name> through *<SEBI Officer Name>* to undertake designated project "*SIT-NET*" Control No *<control no to be communicated by SEBI>*. In this context to ensure that the confidentiality of data is maintained at all the times, it is required that an "Undertaking of confidentiality and non-disclosure" is signed by *<Organization Name>*.

Parties: *"<Recipient Organization>"* through <Recipient Official Name> (**Recipient)** (The Discloser, as may be nominated by SEBI from time to time)

2. The Discloser on the request of the Recipient intends to share access to data records (**the Information**) with the Recipient for the *"SIT-NET*" (**The Project Title**). The Discloser will ensure all data to which access is shared with the Recipient is historical data and adequately anonymized and in no way identifiable to a person. *While adequate care is taken to ensure the privacy of identity, in case Recipient, who has sought access to data stumbles upon such identity implicitly, they should maintain it in confidence.*

3. The Recipient undertakes not to use the Information for any purpose except the stated Purpose. The Source of information would be adequately acknowledged in the research report/paper, if any, published by the Recipient using the information accessed from the Discloser.

4. The Recipient undertakes to keep the Information secure and not to disclose or allow access in any way to any third party and shall maintain its confidentiality in accordance with the terms of this undertaking and as per the law applicable from time to time. The Recipient shall ensure that all data collected, maintained and analyzed by it, are at all times kept secure and fully and effectively protected against unauthorized access or discloser or transmission by accidental or intentional destruction, loss or damage. The Recipient shall adopt and implement appropriate technical and organization security measures to protect data from any kind of unauthorized access by any person including its own employees and would be liable in case of any breach of confidentiality.

5. The undertakings in clauses 2 and 3 above shall apply to all of the Information disclosed by the Discloser to the Recipient, regardless of the way or form in which it is disclosed or recorded but they would not apply to:

   b) any information which is or in future comes into the public domain (unless as a result of the breach of this Undertaking); or

   c) Any information which is already in the public domain.

6. The Recipient shall, at any time on request from the Discloser, return all copies and records of the Information to the Discloser and shall not retain any copies or records of the Information. Any data kept in the computer systems in any format by all the user shall be erased and a confirmation sent to the Discloser, on or before the date as intimated by the discloser.

7. Neither this Agreement nor the supply of any information grants the Recipient any license, interest or right in respect of any intellectual property rights of the Discloser except the right to access and use the Information solely for the stated purpose.

8. In case, the Recipient is an organization, it shall obtain the similar undertaking (for their records) with all the authorized users of the data. The Recipient shall disclose the details of all the users of data of the Recipient organization to the discloser. Any misuse/unauthorized use of information by any of the users of data shall render the Recipient liable under law.

9. The undertakings in clauses 2 and 3 will continue in force indefinitely till such time the confirmation is given under clause 5.The Recipient assumes all legal liability arising out of any precipitative action taken by such Recipient based on the data provided by the Discloser.

10. The Recipient agrees to allow and co-operate with SEBI officials during inspection undertaken to ensure appropriate usage of data or derivative thereof and the Recipient shall abide all the directions/instructions given by the Discloser as regards the usage of the data or derivative(e.g. published paper, training material etc.) thereof.

11. The Recipient agrees that in case it fails to maintain confidentiality of data or fails to abide by any clause of this undertaking or is found indulging in any kind of irregularity with regard to data usage or provides false/misleading information, the Recipient shall be

solely responsible and liable for all actions as per law prevalent at the relevant point of time (Including the law which may came into force after signing this undertaking). Further, the Recipient shall be liable to make good of any loss/damage caused to the Discloser for any unauthorized use/misuse of the information by the Recipient and shall keep the Discloser (and SEBI) indemnified for the same.

	(On Behalf of SEBI)	**Recipient**	
		Authorizing Person (Representing the Organization)	**Recipient Person (Representing the Institute)**
Name			
Signature			
Designation			
Date			

Appendix XII - Detailed list of technologies to be integrated with NOC SOC

To be collected by hand during the RFP bid process.

Appendix XIII - Bill of Material (BOM) for AMC of Existing Network Project

To be collected by hand during the RFP bid process.

Appendix XIV - Bill of Material (BOM) for AMC of Existing Network devices

To be collected by hand during the RFP bid process.

Appendix XV - Existing backup solution of SEBI

SEBI has implemented Veeam backup solution in its private cloud environment. The bidder has to integrate the back up of networking devices and servers with the mentioned Veeam backup solution.

Current version of the Veeam backup solution is 10.0

Appendix XVI - Existing BYOD Policy of SEBI

SEBI’s existing BYOD policy is to be collected by hand during the RFP bid process.