RAILTE CORPORATION OF INIDIA LIMITED

Off: Plot No 143, Sector 44, Institutional Area,
Opposite Gold Souk Mall,
Gurgaon, Haryana122003

Regd.Off: 6thFloor, IIIrd Block, Delhi Technology Park,
Shastri Park, Delhi-110053

Selection of Partner

For

Infra services to RCIL Customer

EOI No: RCIL/EOI/CO/DNM/2019-20/IT SERVICES TO RCIL CUSTOMER/506 dated 23.12.2019

NOTICE

RailTel Corporation of
India Limited
Plot No.-143,
Sector44, Institutional
Area,
Opposite Gold Souk
Mall, Gurgaon,
Haryana -122003

EOI Notice No: RCIL/EOI/CO/DNM/2019-20/IT SERVICES TO RCIL CUSTOMER/506 dated 23.12.2019

RailTel Corporation of India Ltd. (hereafter referred to as RCIL) invites EOIs from the firms, for participating in the process for Partner(s) selection for infra services of RCIL Customer

The details are as under:

1	Discussion with Prospective Partners	27.12.2019 at 10:00 at RailTel Gurgaon office.
2	Last date for submission of EOIs by bidders	31.12.2019 before11:00Hrs.
3	Opening of bidder Response and price bid	31.12.2019 at 11:30Hrs.
4	Number of copies to be submitted for scope of work	One
5	EMD	Rs. 2 Lakh

DD for EMD and should be in the favor of **RailTel Corporation of India Limited** payable at Gurugram.

Prospective bidders are required to direct all communications related to this Invitation for EoI document, through the following Nominated Point of Contact persons:

Contact: Naresh Kumar
Position: Dy. GM/IT
Email:naresh.kumar@railtelindia.com
Telephone: +91124 2714000
Mobile:+91 9717644088

NOTE: **(i) All firms are required to submit hard copy of their EOI submissions, duly signed by Authorized Signatories with Company seal and stamp.**

(ii) Eligible MSMEs are exempted from cost of EOI Documents and EMD, more details are given in clause 14.7 of EOI Document.

1. RailTel Corporation of India Limited–Introduction

RailTel Corporation of India Limited- a "Mini Ratna (Category-I)" PSU Keeping in view the expanding activities in project execution works for telecom and signalling.

In line with the future business plan of RailTel it was felt to diversify into ICT project segment as a System Integrator. Hence, to have clear focus on project execution works, RCIL has been setup. Also this shall help RailTel make a clear distinction between RailTel's existing core activities viz-a-viz project works ensuring resource and accountable separation thereby making RCIL as a separate profit centre. This would also facilitate the Company in proper and suitably reflecting the operational results in a more transparent manner and activity wise.

The aim is to exploit the capabilities and experience gained by RailTel from execution of number of small to large national level projects like National Knowledge Network (NKN), National Optical Fibre Network (NOFN), NE-I & NE-II projects under USOF, and various projects for many other Govt and private agencies. In recent years, RailTel has been expanding its portfolio of services in the areas of Data Centre, Cloud, Telepresence, Retail Broadband (Railwire), etc. With the creation of RCIL, RailTel aims to be one of the leading System Integrator in the country working in the field of ICT.

RCIL shall be taking up turnkey project work for creation, management and operation in the areas of IT, Telecom, networking, Data Center and Railway's ICT and S&T projects. With a dedicated focus and organization suited to executing projects in the areas of expertise, RCIL is poised to become a key driver of growth and innovation for RailTel as well.

****

2. Scope of Work

RailTel is going to participate a Tender floated by PSU for Networking and Security devices. For which RailTel has to engage a empanelled partner to work with RailTel on back to back terms. Detailed of work is enclosed in the EOI.

3. Project Schedule

Detailed project schedule as per details mentioned as per Annexure-8.

4. Minimum Qualification for participation

4.1 The bidder should be empaneled Partner with RailTel.

4.2 The Tenderer/bidder should be an Original Equipment Manufacturer (OEM) or Authorized partner of OEM specifically authorized by OEM for bidding in this tender. The OEM should have proven facilities for Engineering, manufacture, assembly, integration and testing of offered system and basic facilities with respect to space, Engineering, Personnel, Test equipment, Manufacture, Training, Logistic Supports for at least past three years in the country from where the proposed equipment are planned to be supplied.

4.3 The tenderer should present at least one (1) project worth at least 35% of quoted value to showcasing supply, installation, testing, commissioning, implementation and operations projects for Data Center solutions commercially in India in the last 3 years.

4.4 The sum total of the turnover (i.e. revenue from operations) during the last preceding 3 financial years from the date of opening of tender should be Minimum 150% of the quoted value.

4.5 The Tenderer/bidder should have supplied and provision of similar offered security solution with satisfactory working as to Government/PSUs/Telecom Service Providers/Public Listed Company during the last three years from the date of opening of tender.

5. Payment terms

5.1 Payment will be back to back and as per the payment terms mentioned in agreement between RCIL and its customer.

5.2 Payment will be Released after receiving the invoice for the work and after RailTel receives the payment from Customer for the same work.

5.3 Indicative payment term as agreed with customer as under:

S. No.	Payment Schedule	Payment Milestone	Payment (Ref: Annexure-3: Schedule of Rate)
1.	First Instalment	a) Delivery of all the products in good condition and submission of preliminary testing certificate, and b) Submission of Security Deposit and PBG of requisite value and period by RailTel, and verification of the PBG by Railtel from the issuing	70% of the Total Cost of Table-A

S. No.	Payment Schedule	Payment Milestone	Payment (Ref: Annexure-3: Schedule of Rate)
		bank, and c) Submission of documentary proof for ownership of ICT items procured in the name of RailTel Customer, and OEM's documentary proof for Warranty & support Services for all ICT items for a period of five years, and	
2.	Second Instalment	Successful completion and commissioning of the following activities: a) Successful migration, installation of existing hardware from ITC to IDC facility, and its integration with ICT items procured in Table-A of SoR, and b) Successful migration and acceptance of Migration of existing application, including database, currently being managed by RailTel at ITC, and c) Successful migration and acceptance of E-mail servers to IDC, and	i. Remaining 30% of the Total Cost of Table-A, and ii. 100% of the Total Cost of Table-B, excluding Training Cost, and
3.	Third Instalment	Successful completion of Training	100% of Training Cost (item 2 of Table-B)
4.	Post implementation payment	Successful delivery of – a) Managed Services for O&M Services	Payment in arrears on quarterly basis

6. Detailed Schedule of Rates (SOR)

Bidder has quote the Price as per Annexure-3

Note: The bidder has to submit the Rate as per Annexure-3 for five years however contract period will be extendable as agreed with end customer which may increase or decrease as per end customer requirement. Bidder also has to provide the breakup of price of components (storage/servers/firewall/Switch/License etc) as per annexure-3. RCIL may place the order in full or partial manner based on customer requirement. In case of expansion by customer for any component, same price (mention in detail breakup) will be considered for future requirement.

7. Selection criteria

Evaluation will be done on L1 basis of qualified bidder. A pre bid arrangement will be signed with successful partner for participation in the tender. If, RailTel gets the order from customer, back to back order will be placed on quoted price or final negotiated price to the partner for execution and to assist RailTel.

8. SLA's

The service level arrangement will be back to back and all the penalty deducted by Customer will passed on to selected bidder.

9. RCIL’s Right to Accept/Reject Bids

RCIL reserves the right to accept or reject any bid and annual the bidding process or even reject all bids at any time prior to award of contract, without thereby incurring any liability to the affected bidder or bidders or without any obligation to inform the affected bidder or bidders about the grounds for RailTel’s action.

10. Bidding Document

The bidder is expected to examine all instructions, forms, terms and conditions and technical specifications in the bidding documents. Submission of bids, not substantially responsive to the bidding document in every aspect will be at the bidder’s risk and may result in rejection of its bid without any further reference to the bidder.

All pages of the documents shall be signed in ink by the bidder including the closing page in token of his having studies the EOI document and should be submitted along with the bid.

11. Period of Validity of Bid

Bids shall remain valid for a period of 90 days from the date of opening of the bids RCIL shall at its own discretion reject a bid value for shorter period.

12. Bid Currency

The prices in the bid document shall be expressed in Indian Rupees only.

13. Bidding Process (Single Packet System)

The bidding process will consist of single packet system. The detailed technical proposal i.e. the including ‘Price Bid’ shall be submitted in sealed envelope.

14. Security Deposit / Performance Bank Guarantee (PBG)

The successful bidder shall have to submit a performance Bank Guarantee (PBG) within 30 days of the issue of Purchase order @ 5 % of contract value for the satisfactory performance of materials covered in SOR Clause No.-5, valid for a period of 4 months beyond contract period. Extension of time for submission of BG beyond 30(thirty) days and up to 60 days from the date of issue of Letter of acceptance may be given by acceptance Authority . However, a penal interest of 15% per annum shall be charged for delay beyond 60(Sixty) days. i.e from 61st day after issue of LOA.

14.1 The earnest money shall be Released on submission of PBG. If the delivery period gets extended, PBG should also be extended appropriately.

14.2 This PBG would be Released after satisfactory completion of contract.

14.3 No interest shall be paid on the amount of earnest money and Performance Security held by the RCIL, at any stage.

14.4 In case customer demand for any PBG over and above this amount during the contract same will be applicable to the Vendor.

15. Bid Earnest Money (EMD)

15.1 The Bidder shall furnish a sum as given in EOI Notice as Earnest Money in the form of Demand Draft from any scheduled bank in India in favour of “RailTel Corporation of India Limited” payable at Gurgaon which should remain valid for 45 days beyond the bid opening date.

15.2 The EMD may be forfeited if a bidder withdraws his offer or modifies the terms and conditions of the offer during validity period and in the case of a successful bidder, if the bidder fails to accept the Letter of Acceptance (LOA) and fails to furnish performance bank guarantee (security deposit) in accordance with clause 13.

15.3 Offers not accompanied with valid Earnest Money shall be summarily rejected.

15.4 Earnest Money of the unsuccessful bidder will be discharged / returned as promptly as possible but not later than 30 days after the expiry of the period of offer / bid validity prescribed by the Purchaser.

15.5 The successful bidder’s EMD will be discharged upon the bidder’s acceptance of the Advanced purchase order satisfactorily and furnishing the performance bank guarantee in accordance with clause 13.

15.6 Earnest Money will bear no interest.

15.7 For Micro and Small Enterprises (MSEs)

15.7.1 Eligible MSEs are exempted from cost of EOI Documents and EMD.

15.7.2 Certain benefits/preferential treatment shall be extended to the registered MSEs as per guidelines issued in the latest notification of Ministry of MSME/ Government of India.

15.7.3 MSEs who are interested in availing themselves of these benefits will enclose with their offer the proof of their being MSE registered with any of the agencies mentioned in the notification of Ministry of MSME.

15.7.4 The MSEs must also indicate the terminal validity date of their registration.

15.7.5 Failing 10.7.3 and 10.7.4 above, such offers will not be liable for consideration of benefits detailed in the notification of Government of India.

16. Deadline for Submission of Bids

Bids must be submitted to RCIL at the address specified in the preamble not later than the specified date and time mentioned in the preamble. If the specified date of submission of bids being declared a holiday for RCIL, the bids will be received up to the specified time in the next working day.

17. Late Bids

Any bid received by RCIL after the deadline for submission of bids will be rejected and/or returned unopened to the bidder.

18. Modification and/or Withdrawal of Bids

Bids once submitted will treated, as final and no modification will be permitted. No correspondence in this regard will be entertained.

No bidder shall be allowed to withdraw the bid after the deadline for submission of bids.

In case of the successful bidder, he will not be allowed to withdraw or back out from the bid commitments. The bid earnest money in such eventuality shall be forfeited and all interests/claims of such bidder shall be deemed as foreclosed.

19. Details of Financial bid

19.1 The financial bid should clearly bring out the cost of the work with detailed break-up of taxes.

19.2 The financial bid must be submitted as per the enclosed Proforma in EOI document.

20. Clarification of Bids

To assist in the examination, evaluation and comparison of bids the purchaser may, at its discretion, ask the bidder for clarification. The response should be in writing and no change in the price or substance of the bid shall be sought, offered or permitted.

21. Period of Association/Validity of Agreement:

Initial contract will be for five years however based on end Customer requirement same may be extended another 2 years on mutually agreed terms and conditions.

22. Variation in Contract:

+/- 50 % variation may be operated during the period of validity of agreement with the approval of competent authority with similar terms and procedure as specified in the agreement. Contract variation may be used for same Customer for other similar projects after approval of competent authority.

23. Information Security, Compliance and Audit Requirements

23.1 Information Security

a) Bidder shall strictly follow the Information Security Policies, Standards, Procedures and Guidelines of RailTel for colocation and maintenance of Its Customer ICT Infrastructure under scope of this contract.

b) Bidder and its deputed personnel shall not carry and/or transmit any material, information, layouts, diagrams, storage media or any other goods/material in physical or electronic form, that contains data/application details, out of its IDC facility and Internet Ticketing Center without approval of competent authority of RailTel Customer.

c) Bidder shall ensure that all necessary security measures are taken for the physical security of RailTel IDC in order to prevent any un-authorized access to customer applications and data.

d) Bidder shall ensure the confidentiality and integrity of Its Customer ICT Infrastructure collocated in RailTel IDC though complete isolation from other tenant's/client's systems hosted in the same facility.

e) Bidder shall ensure regular and proper backup of customer data as per requirements of customer in order to prevent any data loss.

f) Bidder sRhall, upon termination of this agreement for any reason, or upon demand by RailTel , whichever is earliest, return any and all information provided to the bidder by railTel, including any copies or reproductions, both hardcopy and electronic.

g) Bidder acknowledges that RailTel Customer business data and other proprietary information or materials, whether developed by RailTel Customer or being used by its Customer pursuant to an agreement with a third party (the foregoing collectively referred to herein as "proprietary information") are confidential and proprietary to RailTel Customer; and RailTel agrees to use reasonable care to safeguard the proprietary information and to prevent the unauthorized use or disclosure thereof, which care shall not be less than that used by RailTel to protect its own proprietary information. Bidder recognizes that the goodwill of railtel depends, among other things, upon RailTel keeping such proprietary information confidential and that unauthorized disclosure of the same by Bidder could damage Its Customer, and that by reason of Bidder's duties hereunder. Bidder may come into possession of such proprietary information, even though Bidder does not take any direct part in or furnish the services performed for the creation of said proprietary information and shall limit access thereto to employees with a need to such access to perform the services required by this agreement. Bidder shall use such information only for the purpose of performing the said services.

23.2 **Right to Audit**

a) The ICT Infrastructure of RailTel Customer collocated in RailTel IDC facility shall be subject to regular security audits and compliance assessments, like PCI DSS and ISO 27001 etc. As part of this contract with Bidder , railtel shall reserve the 'Right to Audit' on RailTel IDC Infrastructure, especially audit of Physical Security and Access Control System and related policies and processes.

b) In this regard, Bidder shall ensure that relevant documentation and audit logs, including but not limited to CCTV recordings and Physical Access Control logs, of IDC facility are properly maintained and produced to railTel, or any third-party audit agencies hired by railtel or its customer, for successful compliance against security standard like PCI DSS and ISO 27001.

23.3 **Confidentiality**

a) Bidder shall not use Confidential Information, data, name or the logo of RailTel or Its Customer except for the purposes of providing the Service as specified under this contract;

b) Bidder shall not share any data and/or confidential Information of RailTel or Its Customer, generated, stored, and maintained by Bidder while carrying out the work under this project including any copies or reproductions, both hardcopy and electronic, with any third-party party without explicit approval of competent authority of RailTel or Its Customer.

c) Bidder may only disclose Confidential Information in the following circumstances:

   i. with the prior explicit approval of competent authority of RailTel or Its Customer;

   ii. to a member of the RailTel's Team ("Authorized Person") if:

      - the Authorized Person needs the Confidential Information for the performance of obligations under this contract;
      - the Authorized Person is aware of the confidentiality of the Confidential Information and is obliged to use it only for the performance of obligations under this contract

d) Bidder shall sign a Non-Disclosure Agreement (NDA) with RailTel within 21 days of award of work order. The Bidder, its antecedents, personnel and the sub-contractors shall be bound by the NDA. Bidder will be held responsible for any breach of the NDA by its antecedents, delegates, personnel or sub-contractors. The format of the NDA is provided in Annexure-9: Non-Disclosure Agreement (NDA).

e) In addition to above, Bidder shall also sign an NDA with its sub-contractors, hired by Bidder for providing products or services required under this tender.

f) All manpower/personnel deputed by Bidder for O&M activities under this contract shall also sign NDA with RailTel.

23.4 Background Verification of Personnel

a) Bidder shall depute qualified and experienced personnel to perform the O&M Services under this contract.

b) Bidder shall perform proper and adequate background verification check, including qualification & experience verification and police verification, of all the personnel before deploying them at Customer Location for O&M activities. Bidder shall submit an undertaking to RailTel alongwith copy of verification report, in this regard.

c) This process shall be followed by Bidder for every new personnel deputed for O&M activities under this contract.

23.5 **Statutory Compliance:**

During the tenure of this Contract nothing shall be done by Bidder in contravention of any law, act and/ or rules/regulations, there under or any amendment thereof and shall keep RailTel indemnified in this regard.

Bidder shall comply and ensure strict compliance by his/her employees and agents of all applicable Central, State, Municipal and Local laws and Regulations and undertake to indemnify RailTel or Its Customer from and against all levies, damages, penalties and payments whatsoever as may be imposed by reason of any breach or violation of any law, rule, including but not limited to the claims against RailTel or Its Customer under Employees Compensation Act, 1923, The Employees Provident Fund and Miscellaneous Provisions Act, 1952, The Contract Labour (Abolition and Regulation) Act 1970, Factories Act, 1948, Minimum Wages Act and Regulations, Shop and Establishment Act and Labour Laws which would be amended/modified or any new act if it comes in force whatsoever, and all actions claim and demand arising therefrom and/or related thereto.

23.6 **Exit Management**

As part of Exit Management process, in case the contract with RailTel ends or is terminated before five years, Bidder shall -

a)Return all Customer data and information to RailTel, generated, stored, and maintained by Bidder while carrying out the work under this project including any copies or reproductions, both hardcopy and in electronic from,

b) Provide necessary handholding and transition support to Railtel for maintaining the applications. The handholding support will include but not be limited to, handing over all relevant documentation, system Knowledge transfer, and addressing the queries/clarifications of RailTel with respect to the working / performance levels of the applications etc.

24. Bidder's Information

S.No.	ITEM	Details
1.	Full name of bidder's firm	
2.	Full address, telephone numbers, fax numbers, and email address of the primary office of the organization / main / head / corporate office	
3.	Name, designation and full address of the Chief Executive Officer of the bidder's organization as a whole, including contact numbers and email address	

4.	Full address, telephone and fax numbers, and email addresses of the office of the organization dealing with this EOI	
5.	Name, designation and full address of the person dealing with the EOI to whom all reference shall be made regarding the EOI enquiry. His/her telephone, mobile, Fax and email address	
6.	Bank Details (Bank Branch Name ,IFSC Code, Account number)	
7.	GST registration Number	

25. Format for statement of Deviation

The following are the particulars of deviations from the requirements of the Instructions to bidders:-

S.NO	CLAUSE	DEVIATION	REMARKS (Including Justification)

26. Force Majeure

25.1 If during the Agreement, the performance in whole or in part, by either party, of any obligation under this is prevented or delayed, by reason beyond the control of the parties including war, hostility, acts of the public enemy, civic commotion, sabotage, Act of State or direction from Statutory Authority, explosion, epidemic, quarantine restriction, strikes and lockouts (as are not limited to the establishments and facilities of the parties), fire, floods, earthquakes, natural calamities or any act of GOD (hereinafter referred to as EVENTS), provided notice of happenings of any such EVENT is given by the affected party to the other, within twenty one (21) days from date of occurrence thereof, neither party shall have any such claims for damages against the other, in respect of such non-performance or delay in performance. Provided service under this Agreement shall be resumed as soon as practicable, after such EVENT comes to an end or ceases to exist.

25.2 In the event of a Force Majeure, the affected party will be excused from performance during the existence of the Force Majeure. When a Force Majeure occurs, the affected party after notifying the other party will attempt to mitigate the effect of the Force Majeure as much as possible. If such delaying cause shall continue for more than sixty (60) days from the date of the notice stated above, the party injured by the inability of the other to perform shall have the right, upon written notice of thirty (30) days to the other party, to terminate this Agreement. Neither party shall be liable for any breach, claims, damages against the other, in respect of non-performance or delay in performance as a result of Force Majeure leading to such termination.

27. Settlement of Disputes

26.1 Any dispute or difference whatsoever arising between the parties out of or relating to the construction, meaning, scope, operation or effect of this contract or the validity or the breach thereof shall be settled by arbitration in accordance with the Arbitration and Conciliation Act, 1996 as amended and the award made in pursuance thereof shall be binding on the parties. The venue of such arbitration or proceedings thereof shall be New Delhi.

26.2 All arbitration proceedings shall be conducted in English. Recourse against any Arbitral award so rendered may be entered into court having jurisdiction or application may be made to such court for the order of enforcement as the case may be.

26.3 The Arbitral Tribunal shall consist of the sole Arbitrator appointed by mutual agreement of the parties.

26.4 Each of the parties agree that notwithstanding that the matter may be referred to Arbitrator as provided herein, the parties shall nevertheless pending the resolution of the controversy or disagreement continue to fulfill their obligation under this Agreement so far as they are reasonably able to do so.

28. Governing Laws

The Purchase Order shall be interpreted in accordance with the laws of India. The courts at New Delhi shall have exclusive jurisdiction to entertain and try all matters arising out of this contract.

29. Termination for Default

The purchaser may, without prejudice to any other remedy for breach of contract, by written notice of default, sent to the Tenderer, terminate this contract in whole or in part.

28.1 If the tenderer fails to deliver any or all of the goods within the time period(s) specified in the contract.

28.2 If the tenderer fails to perform any other obligation(s) under the contract; and

28.3 If the tenderer, in either of the above circumstance(s) does not remedy his failure within a period of 30 days (or such longer period as the Purchaser may authorize in writing) after receipt of the default notice from the Purchaser.

28.4 In case of any of the above circumstances the RailTel shall pay the supplier for all products and services delivered till point of termination as per terms and conditions of the contract. However, any recovery and losses occurred to RailTel will be recovered from Contractor up to the value of contract.

30. Clause wise Compliance

Clause wise compliance statement of the Technical Specifications and Commercial Terms & Conditions shall be enclosed with the offer along with the technical literature of the material and other documents in support of relevant clauses.

31. Insurance

The Contractor shall take out and keep in force a policy or policies of insurance from the date, the delivery of material starts (including the transit portion) against all liabilities of the Contractor or the Purchaser. The contractor shall take out and keep in force a Policy or policies of Insurance for all materials covered in schedule of requirement irrespective of whether used up in the portion of work already done or kept for the use in the balance portion of the work until such material are provisionally handed over to RailTel. The goods will be issued by purchaser to supplier and risk of goods shall remain with supplier until the issue of PAC by RailTel. Insurance policy has to be kept valid by the contractor till issue of PAC by RailTel.

The Contractor should insure the stores brought to site, against risks as required under the Emergency Risk (Goods) Insurance Act in force from time to time up to contract value.

It may be noted that the beneficiary of the insurance policy should be RailTel or the policies should be pledged in favor of RailTel. The contractor shall keep the policy/policies current till the equipment are handed over to the purchaser. It may also be noted that in the event of contractor's failure to keep the policy current and alive, renewal of policy will be done by purchaser for which the cost of the premium plus 20% of premium shall be recovered from the contractor.

32. Taxes & Duties

The price quoted in the offer should be firm, fixed indicating the break up and inclusive of all taxes and duties like import, custom, anti-dumping, CGST, IGST, SGST, UTGST etc. The offer should be inclusive of packing, forwarding, freight up to destination, insurance charges.

Bidder shall issue valid tax invoice to RailTel for availing proper credit of CGST/SGST/IGST/UTGST in case of award of contract. GST will not be reimbursed in the absence of valid tax invoice.

For all the taxable supplies made by the vendor, the vendor shall furnish all the details of such taxable supplies in the relevant returns to be filled under GST act.

If the vendor fails to comply with any of the above, the vendor shall pay to purchaser any expense, interest, penalty as applicable under the GST act.

In case of incorrect reporting of the supply made by the vendor in the relevant return, leading to disallowance of input credit to purchaser, the vendor shall be liable to pay applicable interest under the GST act to the credit of purchaser. The same provisions shall be applicable in case of debit/credit notes.

Tenderer shall quote all-inclusive rates, but there shall be break up of basic price and all type of applicable taxes such as SGST/CGST/IGST/UTGST along with respective HSN/SAC code under GST law (Including tax under reverse charges payable by the recipient).

Wherever the law makes it statutory for the purchaser do deduct any amount towards GST at sources, the same will be deducted and remitted to the concerned authority.

The imposition of any new tax and/or increase/ in the aforesaid taxes, duties, levies, after the last stipulated date for the receipt of tender including extensions if any and the bidder there upon necessarily and properly pays such taxes/levies/cess, the bidder shall be reimbursed the amount so paid, provided such payments, if any, is not, in the opinion of RailTel attributable to delay in execution of work within the control of bidder. The bidder shall within a period of 30 days of the imposition of any such tax or levy or cess, give a written notice thereof to RailTel that the same is given pursuant to this condition, together with all necessary information including details of input credit relating thereto. In the event of no payment/default payment of any of the above taxes, RailTel reserves the right to withhold the dues/payments of bidder and make payment to states/central government authorities as may be applicable. However, if the rates are reduced after the last stipulated date for receipt of tender, bidder has to pass on the benefits to RailTel.

In case of imported equipment:

Anti-Dumping duty if applicable on the equipment proposed to be supplied by OEM/Tenderer as per extant instructions of Ministry of Commerce/Finance Government of India, has to be borne by the tenderer and shall be deducted from the amount payable to the bidder at the time of making payment to the firm, if this duty amount is paid to custom Authority by RailTel.

Inter se position of the offers will be determined on total unit rate on CIP destination basis which will include basic rate, custom duty, CGST, SGST, IGST, UTGST, freight, Insurance and any other charges or cost quoted by the tenderer, including GST payable on reverse charge by RailTel, whenever applicable.

In regards to works contract, the tenderer should have registration no. for GST in respective state where work is to be executed and shall furnish GST registration certificate on award of LOA.

33. Other Terms and Condition

Bidders are requested to quote their best prices considering the fact that price negotiation, if required with the customer will be passed on to the selected bidder.

33.1 Unless otherwise specified all prices quoted must remain firm except for statutory variation in taxes and duties during contractual delivery period. Any increase in taxes and duties after expiry of the delivery period will be to vendor account.

33.2 Quotations should preferably be typewritten and any correction or over- writing should be initialled. Rates to be indicated both in words and figures.

33.3 The bidders should furnish a list of its Partners/Directors and a declaration that such Partners/Directors have no interest in any other bidders in respect of the same EOI.

33.4 Sealed quotations in envelope superscribing EOI enquiry number and due date of opening must be sent by Registered or Speed Post or to be dropped in the EOI Box specified for the purpose. Quotations received after specified date and time are liable to be rejected

33.5 Quotation should be valid for a minimum period of 90 days from the date of opening of EOI.

33.6 Printed conditions on the back side of the offers will be ignored.

33.7 GST Registration Number, if any, may be indicated.

33.8 Unless otherwise specified, the materials may be inspected by RCIL after implementation at sites. RCIL may have option to carry out stage inspection/pre-dispatch inspection at Supplier's works.

33.9 Any increase in taxes and duties after expiry of the delivery period will be to supplier's account. This will be without prejudice to the rights of RCIL for any other action including termination.

33.10 RCIL shall have the right to terminate the contract by giving 60 days notice without assigning any reasons thereof. However, in the event of any breach of terms of the contract, RCIL will have right to terminate the contract by written notice to the Seller.

33.11 FORCE MAJEURE: Any delay or failure to perform the contract by either party caused by acts of God or acts of Government or any direction or restriction imposed by Government of India which may affect the contract or the public enemy or contingencies like strikes, riots etc. shall not be considered as default for the performance of the contract or give rise to any claim for damage. Within 7 days of occurrence and cessation of the event(s), the other party shall be notified. Only those events of force majeure which impedes the execution of the contract at the time of its occurrence shall be taken into cognizance.

33.12 In case of any dispute or difference arising out of the contract which can not be resolved mutually between RCIL and vendor, it shall be referred to a Sole Arbitrator to be appointed by the CMD, RCIL,

33.13 The Arbitration and Conciliation Act, 1996 and rules made there under shall apply to the Arbitration Proceedings.

33.14 The contract shall be governed by and construed according to the laws in force in India and subject to exclusive jurisdiction of the Courts of Delhi only.

33.15 RailTel will set up a private/Dedicated Infrastructure for its customer in RailTel Data Center. RailTel will only provide RACK Space and Bandwidth requirement. Supply, Services and O&M as Per scope of work has to be execute by Bidder.

33.16 RailTel will provide clear marking/labeling of its customer infrastructure as per needed RACK space (Full), there should be available space within RACK for upcoming application/server (if any) migration to DC.

33.17 RailTel will Provide Complete access details of servers and storage etc and all other related components including admin rights to be shared with customer support team for monitoring purpose.

33.18 Minimum Contract period for this project will be 5 years.

33.19 Future requirement may be dealt with this methodology only. No exception will be accepted.

33.20 Delivery time 4-6 weeks after confirmed PO.

33.21 Incase customer desire to have a DR for same services same unit rates will be applicable.

****

Annexure-1 COVERING LETTER

COVERING LETTER (To be on company letter head)

EoI Reference No: RCIL/EOI/CO/DNM/2019-20/IT SERVICES TO RCIL CUSTOMER/506 dated 23.12.2019

Date:
To,

Executive Director/DNM
RailTel Corporation of India Ltd.
PlotNo.143, Sector 44, Gurgaon– 122 003

Dear Sir,

SUB: Participation in the EoI process

Having examined the Invitation for EoI document bearing the reference number ____________________ released by your esteemed organization, we, undersigned, hereby acknowledge the receipt of the same and offer to participate in conformity with the said Invitation for EoI document.

If our application is accepted, we undertake to abide by all the terms and conditions mentioned in the said Invitation for EoI document.

We hereby declare that all the information and supporting documents furnished as a part of our response to the said Invitation for EoI document, are true to the best of our knowledge. We understand that in case any discrepancy is found in the information submitted by us, our EoI is liable to be rejected.

We hereby submit EMD of Amount Rs. 2 Lakh through DD dated ______issued from ________ Bank.

Authorized Signatory
Name
Designation

34. List of Documents to be submitted for bidding

1. Covering Letter
2. Format for statement of deviation
3. Format for providing Bidder’s information
4. Commercial Offer
5. Technical Proposal
6. Clause Wise Compliance
7. Signed EOI document
8. Any other Relevant document
9. EMD
10. GST Registration Number

Scope of work

1. Supply, Installation, integration, commissioning and maintenance of ICT Items

1.1. supply, installation, integration, testing, commissioning and maintenance of all ICT Infrastructure items as specified in Annexure-3: Schedule of Rate (SoR). All of these ICT items shall be installed by Bidder in server racks allocated for RailTel Customer in IDC facility.

1.2. Bidder shall be responsible for the tendering and procurement of all ICT items as specified in Annexure-3: Schedule of Rate (SoR). All these ICT items to be procured by Bidder for RailTel Customer under this tender -

a) shall be procured in the name of RailTel Customer. RailTel Customer shall be the owner of all these items. Bidder shall submit the relevant ownership documents to RailTel Customer on the delivery of all these items,

b) shall not become '**End of Support**' before five years from the date of commissioning. Bidder shall obtain necessary undertakings/certificates from all respective OEMs/Software Vendor in this regard and shall submit the same to RailTel Customer.

c) shall be industry-standard products from OEMs of data centre grade ICT solutions, and meet the minimum capacity and performance requirements as specified in Annexure-4: Technical Requirements.

d) shall be at par, in terms of the technical and functional capabilities, with industry standard requirements and data center grade security and best practices.

1.3. Bidder shall ensure that installation, configuration, fine-tuning and integration of all these ICT items are done as per OEM best practices and there shall be no single point of failure in the ICT environment.

1.4. Maintenance of network cabling and labelling of all devices, network and power cabling as per Data Center standards. Bidder shall replace the faulty network cables as and when required. For this Bidder shall maintain adequate stock of network cables.

Note:

i. All software licenses not covered under this tender shall be procured by RailTel Customer and made available to Bidder, alongwith required OEM/Software Vendor Support to enable Bidder carry out the installation and maintenance activities.

ii. If it is observed that any of the ICT items supplied by Bidder under this tender is not able to meet the minimum capacity and performance requirements as stipulated in Annexure-4 during the contract period, Bidder at its own cost shall replace that ICT item with higher end item that meets the minimum capacity and performance requirements.

2. 24x7 Comprehensive Warranty Support and Maintenance Services for Five Years

All the product procured by Bidder for RailTel Customer under this tender shall be bundled with **five years** of Warranty support and maintenance services from respective OEM/Software Vendors.

2.1. The OEM warranty and support services for all ICT items shall be available for a period of **five years** from the date of commissioning of the products or **sixty-six months** from the date of delivery of the products (in case the delay in implementation is on the part of RailTel Customer) whichever is earlier.

2.2. Bidder shall maintain the complete ICT infrastructure in good working condition. The warranty maintenance service shall consist of preventive and corrective maintenance.

2.3. Maintenance coverage will be as per service level requirements defined in Annexure-6: Service Levels & Penalties.

2.4. Bidder shall have necessary tie-ups with the respective OEMs and Software Vendors for the entire period of Warranty support in accordance with the service levels Annexure-6: Service Levels & Penalties.

2.5. The comprehensive warranty support and maintenance services shall cover, but not limited to, the following-

a) There shall be a provision to log complaints/ open support cases directly with OEM on 24 x 7 basis through Phone/Email/Web. Problems in equipment which causes downtime/degradation of services and resolution of which require development of patches, bug fixes etc. shall be treated by OEM on urgent basis. The OEM shall provide appropriate solution on fast-track basis so that desired Service levels are maintained. Bidder shall furnish an undertaking from OEM in this regard along with detailed process document to take support from OEM.

b) Updates and upgrades of operating software, signature database, bug-fixes and patches

c) Resolution of performance related issues and tuning of all supplied software

d) Root Cause Analysis of failures and/or incidents along with OEM recommendations to preclude recurrence of similar failures/incidents in future

e) Guaranteed delivery of spare parts/hardware replacement so as to meet the Annexure-6: Service

Levels & Penalties defined in this tender

f) Configuration support to implement required functionalities and to achieve optimum performance

g) Preventive maintenance in every six months of all network & security equipments supplied by Bidder.

h) Free Upgrades and Updates for equipments as and when released by OEM shall be made available free of cost.

i) All the patches installation and upgrades of network equipments are to be carried out by the Bidder as per the recommendations and releases done by the OEM.

j) All the equipment shall have on-site warranty support i.e. the repair / replacement of faulty units during the warranty period has to be ensured at Bidder IDC.

SLA-based back-to-back support agreement for ‘Warranty Support and Maintenance Services’ shall be signed with the respective OEM. Bidder shall submit the copy of this SLA-based support agreement to RailTel Customer after the delivery of the items.

1. Installation, Configuration, Fine-tuning integration and maintenance of Infrastructure Server

Bidder shall install, configure, fine-tune, integrate, maintain and monitor –

1.1. all the operating systems (both windows and non-windows), including system software/services, for all the servers of RailTel Customer running in both virtualized and physical environments.

1.2. the Redhat Identity Management (IDM) servers in high-availability/cluster mode in virtual environment and integrate the IDM server with all Linux-based servers for centralized user account management, authentication and policy management.

1.3. the Proxy Server and Internal forward-only DNS Server in high-availability, if so required by RailTel Customer, for providing Internet access and DNS resolution to internal servers like application servers.

2. Migration, integration and maintenance of Hardware and Application

A portion of ICT Infrastructure of RailTel Customer hosted at Internet Ticketing Center (ITC) shall be migrated by Bidder to its IDC facility. As part of this, Bidder shall carry out the following activities -

2.1. Insurance, de-installation, packaging, transportation to IDC site, rack mounting, installation, power and data cabling connectivity, and integration of existing hardware (details in Annexure-7) and its integration with ICT infrastructure procured by Bidder for RailTel Customer under this tender. For this, Bidder shall make necessary tie-up with hardware OEM. Bidder shall provide power and data cabling connectivity for these hardware.

2.2. Migration of all RailTel Customer business applications & database, hosted at ITC and managed by Bidder, to IDC facility and its integration with ICT infrastructure at IDC.

2.3. Migration of following Servers and workloads-

a) Email Servers for @RailTel Customer.co.in and @the-maharajas.com domains. For this, Bidder may make necessary tie-up with OEM (M/s Redhat) currently managing these email servers.

b) Email Servers for @RailTel Customer.com domain in co-ordination with IT Team of RailTel Customer Corporate Office.

c) Email Servers for auto-generated transactions emails,

d) Promotional Email Servers (alongwith application and database server for promotional email campaign) in co-ordination with third-party service provider.

e) Transaction and Promotional SMS Servers (deployed by third-party). Bidder shall coordinate with third-party service provide for migration of these servers.

f) Corporate Portal (www.RailTel Customer.com) and ERP Servers of RailTel Customer in co-ordination with IT Team of RailTel Customer Corporate Office.

Migration plan shall be developed by Bidder in co-ordination with RailTel Customer and respective OEM. Bidder shall gather detailed information from RailTel Customer regarding the inventory of assets (hardware and applications) to be migrated, for the purpose of migration plan.

3. Integration Support for the Products/Services procured through Separate Sourcing Process

During the contract period, RailTel Customer may enhance its ICT Infrastructure colocated in RailTel IDC by way of procurement of new products and/or services or up-grade of existing items through third-party vendors. In such case, Bidder shall coordinate with the respective vendor(s) for installation and commissioning of these items, its seamless integration with RailTel Customer ICT infrastructure, and shall maintain the newly procured items in coordination with the vendor. All such ICT items that may be procured by RailTel Customer may include, but not limited to, the following -

3.1. RailTel Customer is in the process of procurement of following hardware items of HPE-make through separate sourcing process.

a) Blade Server Chassis: Qty. 1

b) Blade Servers: Qty. 16

c) Rack-form Servers: Qty. 2

Bidder shall co-ordinate with the respective vendor for rack-mounting, hardware installation, power and network connectivity and its seamless integration with ICT infrastructure procured by Bidder for RailTel Customer under this tender.

3.2. Bidder shall provide full support and co-ordination with third-party service provider for Security Operation Center (SOC) Services for 24/7 log/event monitoring of RailTel Customer ICT Infrastructure at IDC. Bidder shall make necessary configurations on all ICT items of RailTel Customer in its IDC facility for integration with SIEM tools as per recommendations of third-party service provider.

3.3. Bidder shall provide full support and co-ordination with CERT-In and CDAC, or any other agency as per RailTel Customer's requirements, for Security Log/event monitoring of RailTel Customer ICT Infrastructure at IDC. Bidder shall make necessary configurations on all ICT items of RailTel Customer in its IDC facility for integration with SIEM tools as per recommendations of third-party service provider.

a) Disaster Recovery and Business Continuity solutions for RailTel Customer.

4. System Deployment Architecture

The entire ICT Infrastructure of RailTel Customer shall be deployed by Bidder as per indicative System Deployment Architecture specified under Annexure-2: System Deployment Architecture. Bidder shall review and finalize this indicative System Deployment Architecture in coordination with RailTel Customer and respective OEMs/Service providers for deployment of entire ICT Infrastructure, ensuring that no single point of failure exist in the system and deployment is optimized and fine-tuned as per OEM/Industry best practices. Bidder shall document the finalized deployment architecture and get it approved from RailTel Customer before deployment.

4.1. NTP Services

Bidder shall provide Network Time Protocol (NTP) Services through an internal, reliable, secure and accurate time source for network-wide time synchronization of system clocks of all ICT infrastructure of RailTel Customer hosted in Bidder's IDC facility. Bidder shall be responsible for all required security measures to ensure the integrity, security and accuracy of this time source.

5. Operations & Maintenance (O&M) Services

5.1. Scope of on-site O&M Services

Bidder shall providing comprehensive on-site Operations & Maintenance (O&M) of **complete ICT Infrastructure** of RailTel Customer hosted at the following locations -

a) Bidder IDC, and

b) Internet Ticketing Center, RailTel Customer

5.2. On-Site O&M Activities

5.3. On-site O&M Services shall include, but not limited to, the following major activities.

a) IT Help Desk and Fault, Availability and Performance monitoring of complete ICT Infrastructure of RailTel Customer,

b) Hardware Maintenance of complete hardware,

c) System Administration, including Server Virtualization Infrastructure Management, Operating Systems, and Server Software/Services,

d) Application (middleware) Server maintenance for all applications currently being managed by Bidder in RailTel Customer,

e) Database Servers Maintenance,

f) Data Backup and Restoration,

g) Backup Media Management,

h) SAN Storage Maintenance,

i) Network and IT Security Administration,

j) Host Security (Endpoint) Management at Server Layer,

k) Third-party Vendor Management,

l) Coordination for third-party Security Audits,

m) 'Remote Hands Support' at IDC facility,

n) Asset Management (at IDC-facility),

o) MIS Reporting and Documentation.

Refer Annexure-5: Operations & Maintenance Activities and Manpower Details for details.

5.4. Bidder shall carry out the on-site O&M activities from Internet Ticketing Centre (ITC) office of RailTel Customer as under-

a) Remote Infrastructure Management: O&M services of the ICT Infrastructure at IDC shall be carried out remotely from Internet Ticketing Center. All engineers shall work on-site from RailTel Customer Internet Ticketing Center office at State Entry Road.

b) Bidder shall provide 'Remote Hand Support' at IDC through its Data Center staff for physical support for rack mounting, installation, part replacement/repair, network and power connectivity, labelling, troubleshooting and hardware maintenance of RailTel Customer ICT Infrastructure.

c) Any of the on-site engineers deputed at ITC may be asked by RailTel Customer to visit IDC site On need basis or in emergency. This will be without any extra cost to RailTel Customer.

5.5. On-Call On-Site Level-3/Expert Level Support

a) In addition to providing full time on-site technical resource, Bidder shall also align its Level-3/Expert Level resources on On-Call and On-site basis, at Internet Ticketing Center and/or IDC facility, for technical support on all the Products & Services supplied by Bidder under this tender in circumstances including, but not limited to, the following:

i. Troubleshooting, diagnosis and resolution of issues/problems/ Performance degradation with root cause analysis which on-site team is not able to address.

ii. Installation, re-installation, hardware replacement, performance-tuning, OS/application version/firmware or patch upgrades

iii. Non-routine expert-level/advance configuration changes for which on-site team do not have required skill set and experience

iv. Preventive maintenance, in coordination with on-site engineer.

b) Such support shall be asked by RailTel Customer as and when required on need basis only. RailTel Customer reserves the right to decide when such support is required and the same shall be provided by Bidder.

c) If approved by RailTel Customer, Bidder can be allowed to provide such support remotely through reliable and secure remote session/Webex/Web conferencing service in the presence of on-site engineer. However, in case on-call support through remote session is not approved by RailTel Customer, Bidder shall make such support available on-site basis without delay.

5.6. IT Service Management

a) Bidder shall implement a centralized IT Help Desk for RailTel Customer as per IT Service Management best practices for O&M. For this, Help Desk solution shall be procured and implemented by Bidder under this tender.

b) Following minimum processes shall be Bidder shall develop and implement the following, but not limited to, processes as per RailTel Customer requirements for IT Service Management

i. Incident Management

ii. Change Management

iii. Knowledge Management

iv. Service Level Management

v. Request Fulfilment

c) Helpdesk will act as the central point of contact among O&M teams, application team, third-party service providers as well as internal-users of RailTel Customer on a day-to-day basis. Helpdesk will also be a focal point for Incidents management, Change management, Knowledge Maangement and Service Requests. The helpdesk should be able to inform RailTel Customer of all relevant service events, actions and service changes that are likely to affect them. Helpdesk shall provide end to end ownership of the calls/incidents till resolution.

d) Bidder shall manage all Incidents and Change Logs/Trail through Help Desk. For this, required workflows shall be designed and implemented by Bidder using Help Desk tools.

5.7. Preventive Maintenance:

Bidder shall carry out the preventive maintenance once a year for all hardware or equipment supplied by Bidder under this tender, in off-peak hours, which will include the following:

a) Diagnostic tests to check and verify good health of all network and security equipment (CPU and/or other processors, RAM, Flash memory, NV RAM, network ports, various functional modules etc.)
b) Shall use diagnostic software or alternative facility/facilities to diagnose and analyse predictive failures in the disk drive.
c) Perform physical inspection to see that all peripheral devices are in no fault condition.
d) If any fault is detected during diagnostics then take necessary steps to rectify it and replace it, if required.
e) Analyse error log for errors reported since previous Preventive Maintenance activity.
f) If any errors are observed in error log, analyse them in detail and carry out necessary activities to eliminate them.
g) Collect data for all controllers and record in the site log
h) Preventive Maintenance (PM) report, which highlights the findings & follow-up actions, will be furnished to RailTel Customer within one week.

5.8. Manpower for O&M Services

a) Bidder shall deploy following minimum technically qualified engineers to carry out the O&M services on 24/7 basis:

#	Support Level	Manpower	No. of shifts	Min. person in Shift	Min. Qualification and Skills	Minimum Experience
1	L1	Help Desk (L1)	3 – on all days	1	Engineer/ MCA Basic Knowledge of hardware, Operating system, Networking etc.	1 Year of monitoring and maintenance of IT infrastructure
2	L2	System Administrator for System (OS	3 – on all days	2	Engineer/ MCA Trained/Certified in Server Operating System (non-	3 years of hands-on experience in operating

		layer), Server Software and Middleware Maintenance			windows) and middleware	system and server software (web/app etc.) hosted in data center environment.
3	L2	Network and IT Security Engineer	3 – on all days	2	Engineer/ MCA Trained/Certified in deployed network and IT Security technologies	3 years of hands-on experience in network and IT Security technologies hosted in data center environment.
4	DBA	Database Administrator for Database Maintenance	3 – on all days	1	Engineer/ MCA Oracle Certified Professional (OCP)	3 years of hands-on experience on Oracle RDBMS and RAC hosted in data center environment
5	L3	**Remote Team – identified by Bidder for each area of specialization – for all ICT items supplied and implemented by Bidder**				

b) In addition to above manpower, Bidder shall also deploy one full-time on-site Project/Operation Manager at RailTel Customer who will act a Single Point of Contact (SPoC) for RailTel Customer and supervise the entire O&M team for smooth operations & maintenance related matters.

c) The number of manpower can be increased or decreased during the contract period on the basis of system workload and skill-set requirements, as per mutual agreement between RailTel Customer and Bidder

d) Bidder shall submit documents/certifications of qualifications, work experience, and background verification of all the engineers before deputing them at RailTel Customer. All such documents shall be attested by authorized signatory of Bidder.

e) RailTel Customer reserves the right to conduct the screening of all engineers, deputed by Bidder for O&M, in terms of qualifications, experience, key competencies and certifications requirements and reject any engineers who is found non-eligible.

f) At any time during the service period, RailTel Customer may ask Bidder to replace any of the engineers immediately or as deemed fit by RailTel Customer, on ground including but not limited to technical in-competencies, irregularity/non-punctuality in duty, violation of RailTel Customer policies or procedures or contract rules and undisciplined behaviour etc.

g) All engineers shall log attendance (both arrival and departure time) on daily basis using RailTel Customer's Bio-metric Attendance Monitoring system. The Operation manager shall maintain the attendance record and time sheet (details of tasks/activities performed by on-site resources) for all staff.

h) Bidder shall provide adequate training to its technical resources deputed on-site for operations & maintenance of all IT items procured and installed for RailTel Customer under this tender.

In case RailTel Customer procure any new technology/product/services for its ICT Infrastructure through separate sourcing process during the contract period, on-site hands-on training shall be arranged by RailTel Customer for on-site engineers of Bidder for the O&M. After installation of such technology/product/services, the same shall be covered under on-site O&M scope and on-site engineer shall maintain the same in coordination with respective third-party vendor.

i) Bidder and its personnel/representative shall not alter / change / replace any hardware component proprietary to RailTel Customer and/or under warranty or AMC of third party without prior consent of RailTel Customer.

j) Bidder and its personnel/representative shall not install any hardware or software without consent of RailTel Customer.

6. Training

Bidder shall provide hands-on training related to administration, operations and maintenance of the following items on-site at Internet Ticketing Center or Training facility of OEM/bidder. Official Training material shall be provided to a minimum of 4 participants.

S. No.	Topic	No. of Days
	Network Firewalls	As per OEM's Official Training Program
	Anti-APT Solution	
	Application Delivery Controller, including Web Application Firewall	
	Privileged Identity Management	
	Two-factor Authentication	
	Server Virtualization	

7. **Documentation**

a) Bidder shall maintain a Site Management Guide for entire ICT Infrastructure of RailTel Customer colocated at IDC facility.

b) For system integration and installations, Bidder shall develop all necessary documentation, review these with RailTel Customer and responsive OEMs/vendor, and finalize the same after approval of RailTel Customer. Such documentation may include, but not limited to the following-

i. Final System Deployment Architecture.

ii. Server Rack layout diagram

iii. Network diagrams – logical and physical, and cabling layout diagram

c) Submission of all the Supporting Documentation (Design Documents, Installation and Configuration Procedure, Validation Workbook)

d) As part of operations and maintenance services, the Bidder shall maintain all such documents with proper version control. All O&M activities shall be well documented by the Bidder. This will also be required by RailTel Customer for compliance purpose.

Annexure-2: System Deployment Architecture

System Deployment Architecture

This architecture shall be reviewed and finalized with low level design details by RailTel in consultation with respective OEMs/vendors and RailTel Customer. ICT Infrastructure will be deployed as per finalized architecture after approval of RailTel Customer.

Salient features of the Network Architecture are given as under:

a) The entire set of ICT equipment/s shall be deployed in **High Availability** mode to preclude single point of failure.

b) The entire ICT Infrastructure of Data Center will be IPv6 ready (dual stack with both IPv4 and IPv6) from day one.

c) Dedicated zones (i.e. DMZ and MZ) for entire ICT Infrastructure for high performance and security. Servers wi be deployed in multiple zones such as Web servers and Mail servers in DMZ, Application servers, DB servers and other servers like SMS Server, Reporting Server, Management servers, etc. in MZ in the Data Centre. This ensures that infrastructure that is not required to be publicly accessible is well protected and secure.

d) Separate network zones for PCI complaint systems – **PCI DSS Zone** – both at DMZ and MZ layers.

e) Multi-layered network security with Front-end & Back-end Firewalls, NIPS, Web Application Firewall, Privileged Identity Management, VPN and Two-factor authentication etc.

f) Application Delivery Controllers (ADCs) for implementing various network functions like SSL Offloading, Web Application Firewall (WAF), Server Load Balancing (SLB), TCP optimization, Caching etc. ADCs will be used for balancing concurrent sessions across multiple web servers. Similarly, the same system may be planned for load balancing of traffic for other services like email etc.

g) Two-tier Data center network topology with Core and Access Layers. Core layer for DMZ and MZ shall be built with Layer-3 10G switches. Access layer shall be built with Layer-2 Network Switches and Blade chassis switches

h) Non-blocking 10 Gigabit LAN Switching fabric for high performance.

i) Spanning Tree Protocol (STP) free network architecture using technologies like MC-LAG/Virtual Chassis/stacking at Core Layer and Stacking at Access Layer.

j) Internet bandwidth in redundancy from at least two different ISPs. BGP peering with ISPs on IPv4 and IPv6 public IP pool obtained by RailTel Customer from IRINN.

k) Multiple Point-to-point Leased lines connectivity with redundancy through dynamic routing protocol.

l) Network-wide time synchronization through NTP Servers.

Server Virtualization Infrastructure

a) Most of the IT Infrastructure workload will be virtualized on Server Virtualization solution including, but not limited to the following:
   - Web Servers
   - Application Servers
   - Email Servers
   - Privileged Identity Management (PIM) Servers
   - Secure Email Gateway
   - Internal DNS Servers
   - Staging/Testing Servers on RHEL/Windows OS
   - Patch Management Servers
   - EMS (Help Desk, Network Management Servers)
   - Anti-Virus Server for Server
   - Internet Proxy (like squid) Servers
   - Redhat Identity Management Server
   - Any other workload as and when required by RailTel Customer during service contract period.

b) Separate virtual clusters will be implemented for VMs running in DMZ and MZ zones. One physical server will run either DMZ VMs or MZ VMs, and not both.

c) Virtualization Manager Module will be deployed in high availability to preclude any single point for failure.

d) All virtual machines images for virtual environment will be maintained in SAN storage. For this, all such servers running as hosts for virtual machines will be connected to SAN storage for centralized storage for all virtual machines and related data.

e) Server virtualization shall be configured, fine-tuned and optimized for high level of availability and reliability with High Availability (HA), Live Migration, VM templates & Clones, VM backup etc.

User Authentication, Policy Management and Access Control:

- Redhat Identity Management Server:
  - It shall act as a Centralized User Repository for user authentication, policy management for non-windows servers.
- Privileged User Access Management
  - Privileged Identity Management (PIM) solution shall be implemented to manage Privileged users (administrator/root users) access to critical ICT Infrastructure devices
  - PIM solution shall be deployed in high availability in software/virtual appliance form in virtual environment.
  - PIM solution may be integrated with Redhat IDM Server/Active Directory for centralized user authentication.
- Remote Access:
  - Remote Access of RailTel Customer internal application/resources from Internet for RailTel Customer employees through SSL VPN Servers.
  - Remote access to RailTel Customer Infrastructure for root/admin users will be provided through VPN with two-factor authentication

Email Security

- Secure Email Gateway (SEG) solution shall be used for scanning and filtering of inbound emails for spam, phishing and malicious emails before forwarding the emails to RailTel Customer E-mail servers.

Web Security

- All website/web applications will be configured to run on HTTPS with TLS 1.2 or above
- Inspection of Inbound and outbound web traffic through Web Application Firewall

SSL/Traffic

- Entire inbound SSL/TLS traffic shall be inspected (SSL Inspection) by IPS module at NGFW (Perimeter) and finally off-loaded at ADC in DMZ before WAF inspection.

Host Security

- Host security solution (AV + HIPS + Host Firewall) shall be implementer at Server level

Mail Servers for Business Applications & Services

Multiple instances of different types of mail servers will be deployed on RHEL Postfix, including but not limited to the following–

- Type-1: Mail Stores - Mail servers hosting mailboxes for various domains including
    - @RailTel Customer.co.in for hosting mailboxes for E-ticketing and other services including E-Ticketing Customer Care (in cluster mode) on HTTP/s (webmail), IMAP/PoP3
    - @the-maharajas.com for hosting mailboxes for Maharajas Express Luxury Train services (in standalone/cluster) on HTTP/s (webmail), IMAP/PoP3.
    - @RailTel Customer.com for hosting mailboxes for RailTel Customer Corporate users.
- Type-2: Outgoing Mails Servers without mailbox
    - Auto-generated Transaction Emails - Mail servers (SMTP only) instance for sending auto-generated transactions details to transacting customer. Auto-generated transactions mails will be generated by the application servers to the mail queues of auto-generated mail server.
    - Promotional Mail servers - Multiple instances of mail servers (SMTP only) instance for sending business promotional e-mails to RailTel Customer registered users. Email contents for promotional mails and auto-generated transactions mails will be generated by mailer database server to the mail queues of promotional mail servers.

SMS Servers

- SMS Server(s) would be deployed and managed by third-party service provider and will be integrated with RailTel Customer application/database servers for sending SMS to registered/transacting users.
- These SMS servers may also be used for integration with 2FA solution for sending OTP SMS for two-factor authentication.

Annexure-3: Schedule of Rate (SoR)

Schedule of Rate (SoR)

Table A: ICT Items (Network & Security Equipments, Hardware, Software and Cabling Components) bundled with Five years of OEM Warranty Support

#	Items	Qty.	Make & Model	Unit Cost	Total Cost	Taxes Amt.	Total Cost including taxes
1.	Network Routers (Internet Gateway)	2					
2.	Network Routers (WAN Aggregation)	2					
3.	48-Port Network Switches (Layer-3)	4					
3.1.	SFP+ Transceivers (10G)	96					
3.2.	SFP Transceivers (1G)	16					
4.	Network Switches (Layer-2)	12					
5.	Next Generation Firewall with Threat Prevention (Perimeter)	1:1 HA					
6.	Next Generation Firewall (Internal)	1:1 HA					
7.	Anti-APT Solution	1:1 HA					
8.	Application Delivery Controller (ADC) with Web Application Firewall	1:1 HA					
9.	Privileged Identity Management (PIM) Solution alongwith required OS and DB	1:1 HA					
9.1.	Device Licenses	Min. 50					
9.2.	Privileged User Licenses	Min. 50					
10.	Two-factor Authentication Solution alongwith required OS and DB	1					
10.1.	Concurrent User Licenses	Min.100					
11.	Secure Email Gateway Virtual Appliance	1500 Users					
12.	Server Virtualization Solution	1					
12.1.	Per Two-Physical Socket License	16					
13.	NMS Solution alongwith required OS and DB	1					
13.1.	Fault, Performance & Availability Monitoring Licenses	250					
13.2.	Network Configuration Management Licenses	50					
13.3.	Network Traffic Analysis Licenses	10					
13.4.	Application Monitoring Licenses (Application/Process/Services/URL Monitoring)	100					
14.	Help Desk Solution alongwith required OS and DB	1					
14.1.	Concurrent Help Desk Agent Licenses	2					
15.	Passive Components - Network Cabling and Accessories, including Cables, Labels etc. for	Lot					
	Total Cost						

Table B: One-time Services

#	Items	Qty.	Cost	Taxes Amt.	Total Cost including taxes
1.	Installation Services for all items in Table-A	Lumpsum			
2.	Migration Charges for existing hardware at ITC (Servers, Blade Chassis, SAN Storage System and Tape Library of HPE make)	Lumpsum			
3.	Migration of existing application, including database, currently being managed by RailTel at Internet Ticketing Center	Lumpsum			
4.	Migration Charges for existing email servers and data for following email servers • @xx.co.in • @the-maharajas.com	Lumpsum			
5.	Training Charges for ICT items	Lumpsum			
	Total Cost				

Table C: Cost of Operations & Maintenance (O&M) Services

#	Items	First three years cost	4th year cost	5th year cost	Total Five year cost	Taxes Amt.	Total Cost including taxes
1.	System Administrators						
2.	Network & IT Security Engineers						
3.	Database Administrators						
4.	Help Desk						
	Total Cost						

Table-G: Grand Total Cost	**Amount including taxes**
Grand Total Cost including taxes = (Sum of Total Cost of Table A + B + C)	
In Words:	

Optional items:

#	Item	Unit	Amount excluding taxes
1.	AMC for all supplied ICT items (Table-A) for 6th year	Lumpsum	
2.	AMC for all supplied ICT items (Table-A) for 7th year	Lumpsum	

Signature …..............…………

Name of the Authorized Signatory……........……………

Designation: ………………………

Company Seal ……….........…………

Note:

a) Bidder shall provide the cost breakup with component wise rates for all items in Table-A. These components wise rates may be used by RailTel for any upgrade requirements in future during the contract period.

b) Bidder shall provide the Cabling cost breakup with unit cost of each type of optical and UTP cabling and accessories as required for this project.

Annexure-4: Technical Requirements

Note:

a) All equipments shall be standard 19-inch rack mountable.

b) All products shall be IPv6 Ready supporting dual stacking (IPv4 and IPv6) from day one.

c) All products, except Two-Factor Authentication solution, shall be deployed in high availability to preclude any single point of failure.

d) Any product shall not become **'End of Support'** before **Five years** from the date of commissioning.

e) Installation, Configuration, and optimization of all products shall be done as per OEM best practices.

f) All the products procured and supplied by Bidder shall be compatible with existing equipments currently installed at RailTel Customer ITC and to be migrated to IDC.

g) 10G Network shall be implemented on Optical fibre cabling whereas 1G network shall be on UTP cabling

h) Type of cabling and network interfaces shall be as per Data Cabling Standard of RailTel IDC and compatible with Servers and SAN storage systems (HP make), procured by RailTel Customer through separate sourcing process, which will be integrated by Bidder with these network and security infrastructure items. For this, Biddrer shall gather details of networking interface, cabling and power system requirements of these servers and storage items from RailTel Customer.

i) All software solutions including PIM, 2FA NMS, Help Desk etc., should be complete in all respects i.e. including software, underlying OS license, Database license etc. as part of complete solution.

(NGFW Perimeter)

Feature	Technical Specification
Industry recommendations	The Firewall solution offered must be rated as 'leaders' in the latest Magic Quadrant for Enterprise Firewall published by Gartner from last 2 years
Hardware Architecture	The appliance based security platform should provide firewall, AVC, IPS, Anti-APT and VPN (Site to Site and Remote Access) functionality in a single appliance from day one
	The appliance should support atleast 8 * 1G Gigabit ports and 4 x 10G SFP+ from day one and should be scalable to additional 8 * 10G in future.
	The appliance hardware should be a multicore CPU architecture with a hardened 64 bit operating system to support higher memory and should support minimum of 128 GB of RAM or more
	Proposed Firewall should not be proprietary ASIC based in nature & should be open architecture based on multi-core cpu's to protect & scale against dynamic latest security threats.
	The proposed solution shouldn't use a proprietary ASIC hardware for any kind of performance Improvement. If option to disable ASIC is there than OEM must mention the performance numbers in datasheet
Performance & Scalability	Should support 5 Gbps of NGFW (FW, AVC, IPS, URL filtering, Anti-APT) real-world / production / Enterprise Testing performance / 64K HTTP / 1024B HTTP
	Firewall should support atleast 10,000,000 concurrent sessions or more

	Firewall should support atleast 200,000 connections per second or more
	Firewall should have integrated redundant hot-swappable power supply
	Firewall should have integrated redundant hot-swappable fan tray / modules
NG Firewall Features	Firewall should support creating access-rules with IPv4 & IPv6 objects, user/groups, application, geolocation, url, zones, vlan, etc
	Firewall should support static nat, dynamic nat, dynamic pat
	Firewall should support Nat66 (IPv6-to-IPv6), Nat 64 (IPv6-to-IPv4) & Nat46 (IPv4-to-IPv6) functionality
	Should support Static, RIP, OSPF, OSPFv3 and BGP, BGPv6
	Should support Multicast protocols like IGMP, PIM, etc
	Should support capability to integrate with other security solutions to receive contextual information like security group tags/names
	Should have the capability of passively gathering information about virtual machine traffic, network hosts and their activities, such as operating system, services, open ports, client applications, and vulnerabilities, to assist with multiple activities, such as intrusion event data correlation, elimination of false positives, and policy compliance.
	Should support more than 3000 (excluding custom application signatures) distinct application signature as application detection mechanism to optimize security effectiveness and should be able to create 40 or more application categories for operational efficiency
	Should be capable of dynamically tuning IDS/IPS sensors (e.g., selecting rules, configuring policies, updating policies, etc.) with minimal human intervention.
	Should support more than 15,000 (excluding custom signatures) IPS signatures or more.
	Should be capable of automatically providing the appropriate inspections and protections for traffic sent over non-standard communications ports.
	Should be able to link Active Directory and/or LDAP usernames to IP addresses related to suspected security events.
	Should be capable of detecting and blocking IPv6 attacks.
	The solution should be able to identify, decrypt and evaluate both inbound and outbound SSL traffic on-box
	Should support the capability to quarantine end point by integrating with other security solution like Network Admission Control
	Solution should support full-featured NBA capability to detect threats emerging from inside the network. This includes the ability to establish “normal” traffic baselines through flow analysis techniques (e.g., NetFlow) and the ability to detect deviations from normal baselines.
	The solution must provide IP reputation feed that comprised of several regularly updated collections of poor repuration of IP addresses determined by the proposed security vendor
	Solution must support IP reputation intelligence feeds from third party and custom lists of IP addresses including a global blacklist
	Should must support DNS threat intelligence feeds to protect against threats
	The Appliance OEM must have its own threat intelligence analysis center and should use the global footprint of security deployments for more comprehensive network protection.
	The detection engine should support capability of detecting and preventing a wide variety of threats (e.g., network probes/reconnaissance, VoIP attacks, buffer overflows, P2P attacks, etc.).
	Should be able to identify attacks based on Geo-location and define policy to block on the basis of Geo-location
	The detection engine must incorporate multiple approaches for detecting threats, including at a minimum exploit-based signatures, vulnerability-based rules, protocol anomaly detection, and behavioral anomaly detection techniques.
	Should support Open based Application ID / Custom Application ID for access to community resources and ability to easily customize security to address new and specific threats and applications quickly
URL Filtering	Should support Reputation- and category-based URL filtering offering comprehensive alerting and control over suspect web traffic and enforces policies on more than 280 million of URLs in

	more than 80 categories.
Anti-APT / Malware Features	Should support the capability of providing network-based detection of malware by checking the disposition of unknown files using SHA-256 file-hash or signature as they transit the network and capability to do dynamic analysis on-premise on purpose built-appliance
	Solution shall have capability to analyze and block TCP/UDP protocol to identify attacks and malware communications. At minimum, the following protocols are supported for real-time inspection, blocking and control of download files: HTTP, SMTP, POP3, IMAP, NetBIOS-SSN and FTP
	Proposed solution shall have required subscription like Threat Intelligence for proper functioning
	Local Malware analysis appliance shall be capable of executing MS Office Documents, Portable Documents, Archive Files, Multimedia Files and executable binaries or more in a virtual environment.
	Local Malware analysis appliance shall have integrated redundant power supply and minimum of 2 x 10 Gig ports or more
Management	The management platform must be accessible via a web-based interface and ideally with no need for additional client software
	The management platform must be a dedicated OEM appliance and VM running on server will not be accepted
	The management appliance should have 2 x 10G port and integrated redundant power supply from day one
	The management platform must be able to store record of 15000 user or more
	The management platform must provide a highly customizable dashboard.
	The management platform must domain multi-domain management
	The management platform must provide centralized logging and reporting functionality
	The management platform must be capable of integrating third party vulnerability information into threat policy adjustment routines and automated tuning workflows
	The management platform must be capable of role-based administration, enabling different sets of views and configuration capabilities for different administrators subsequent to their authentication.
	Should support troubleshooting techniques like Packet tracer and capture
	Should support REST API for monitoring and config programmability
	The management platform must provide multiple report output types or formats, such as PDF, HTML, and CSV.
	The management platform must support multiple mechanisms for issuing alerts (e.g., SNMP, e-mail, SYSLOG).
	The management platform must provide built-in robust reporting capabilities, including a selection of pre-defined reports and the ability for complete customization and generation of new reports.
	The management platform support running on-demand and scheduled reports
	The management platform must risk reports like advanced malware, attacks and network
	The management platform must include an integration mechanism, preferably in the form of open APIs and/or standard interfaces, to enable events and log data to be shared with external network and security management applications, such as Security Information and Event Managers (SIEMs), and log management tools.
	Proposed solution should support 24x7x365 OEM TAC support and advance Next Business Day Hardware replacement

(NGFW Internal)

Feature	Technical Specification
Industry	The Firewall solution offered must be rated as ‘leaders’ in the latest Magic Quadrant

recommendations	for Enterprise Firewall published by Gartner from last 2 years
Hardware Architecture	The appliance based security platform should provide firewall, AVC, and IPS functionality in a single appliance from day one
	The appliance should support atleast 8 * 1G Gigabit ports and 4 x 10G SFP+ from day one and should be scalable to additional 8 * 10G in future.
	The appliance hardware should be a multicore CPU architecture with a hardened 64 bit operating system to support higher memory and should support minimum of 64 GB of RAM or more
	Proposed Firewall should not be proprietary ASIC based in nature & should be open architecture based on multi-core cpu's to protect & scale against dynamic latest security threats.
	The proposed solution shouldn't use a proprietary ASIC hardware for any kind of performance Improvement. If option to disable ASIC is there than OEM must mention the performance numbers in datasheet
Performance & Scalability	Should support 5 Gbps of NGFW (FW, AVC, and IPS) real-world / production / Enterprise Testing performance / 64K HTTP / 1024B HTTP
	Firewall should support atleast 3,000,000 concurrent sessions or more
	Firewall should support atleast 50,000 connections per second or more
	Firewall should have integrated redundant hot-swappable power supply
	Firewall should have integrated redundant hot-swappable fan tray / modules
NG Firewall Features	Firewall should support creating access-rules with IPv4 & IPv6 objects, user/groups, application, geolocation, url, zones, vlan, etc
	Firewall should support static nat, dynamic nat, dynamic pat
	Firewall should support Nat66 (IPv6-to-IPv6), Nat 64 (IPv6-to-IPv4) & Nat46 (IPv4-to-IPv6) functionality
	Should support Static, RIP, OSPF, OSPFv3 and BGP, BGPv6
	Should support Multicast protocols like IGMP, PIM, etc
	Should support capability to integrate with other security solutions to receive contextual information like security group tags/names
	Should have the capability of passively gathering information about virtual machine traffic, network hosts and their activities, such as operating system, services, open ports, client applications, and vulnerabilities, to assist with multiple activities, such as intrusion event data correlation, elimination of false positives, and policy compliance.
	Should support more than 3000 (excluding custom application signatures) distinct application signature as application detection mechanism to optimize security effectiveness and should be able to create 40 or more application categories for operational efficiency
	Should be capable of dynamically tuning IDS/IPS sensors (e.g., selecting rules, configuring policies, updating policies, etc.) with minimal human intervention.
	Should support more than 15,000 (excluding custom signatures) IPS signatures or more.
	Should be capable of automatically providing the appropriate inspections and protections for traffic sent over non-standard communications ports.
	Should be able to link Active Directory and/or LDAP usernames to IP addresses related to suspected security events.
	Should be capable of detecting and blocking IPv6 attacks.
	The solution should be able to identify, decrypt and evaluate both inbound and outbound SSL traffic on-box
	Should support the capability to quarantine end point by integrating with other security solution like Network Admission Control
	Solution should support full-featured NBA capability to detect threats emerging from inside the network. This includes the ability to establish “normal” traffic baselines through flow analysis techniques (e.g., NetFlow) and the ability to detect deviations

	from normal baselines.
	The solution must provide IP reputation feed that comprised of several regularly updated collections of poor repuration of IP addresses determined by the proposed security vendor
	Solution must support IP reputation intelligence feeds from third party and custom lists of IP addresses including a global blacklist
	Should must support DNS threat intelligence feeds to protect against threats
	The Appliance OEM must have its own threat intelligence analysis center and should use the global footprint of security deployments for more comprehensive network protection.
	The detection engine should support capability of detecting and preventing a wide variety of threats (e.g., network probes/reconnaissance, VoIP attacks, buffer overflows, P2P attacks, etc.).
	Should be able to identify attacks based on Geo-location and define policy to block on the basis of Geo-location
	The detection engine must incorporate multiple approaches for detecting threats, including at a minimum exploit-based signatures, vulnerability-based rules, protocol anomaly detection, and behavioral anomaly detection techniques.
	Should support Open based Application ID / Custom Application ID for access to community resources and ability to easily customize security to address new and specific threats and applications quickly
Management	The management platform must be accessible via a web-based interface and ideally with no need for additional client software
	The management platform must be a dedicated OEM appliance and VM running on server will not be accepted
	The management appliance should have 2 x 10G port and integrated redundant power supply from day one
	The management platform must be able to store record of 15000 user or more
	The management platform must provide a highly customizable dashboard.
	The management platform must domain multi-domain management
	The management platform must provide centralized logging and reporting functionality
	The management platform must be capable of integrating third party vulnerability information into threat policy adjustment routines and automated tuning workflows
	The management platform must be capable of role-based administration, enabling different sets of views and configuration capabilities for different administrators subsequent to their authentication.
	Should support troubleshooting techniques like Packet tracer and capture
	Should support REST API for monitoring and config programmability
	The management platform must provide multiple report output types or formats, such as PDF, HTML, and CSV.
	The management platform must support multiple mechanisms for issuing alerts (e.g., SNMP, e-mail, SYSLOG).
	The management platform must provide built-in robust reporting capabilities, including a selection of pre-defined reports and the ability for complete customization and generation of new reports.
	The management platform support running on-demand and scheduled reports
	The management platform must risk reports like advanced malware, attacks and network
	The management platform must include an integration mechanism, preferably in the form of open APIs and/or standard interfaces, to enable events and log data to be shared with external network and security management applications, such as Security Information and Event Managers (SIEMs), and log management tools.

	Proposed solution should support 24x7x365 OEM TAC support and advance Next Business Day Hardware replacement

(APT)

S.No	Technical Specifications
	Malware Analysis Appliance
1	The Sandbox solution must support capability to detect both known and unknown malware behaviors.
2	The Sandbox solution must be able to work with proposed NGFW and Email security systems
3	The Proposed solution must provide a detailed analysis of the effect of the malware on systems
4	A hash of the malware should be created for tracking purposes and should support MD5, SHA1 and SHA256 lookups
5	The malware analysis /Sandbox solution should not use any instrumentation or modify any operating system environment capabilities to monitor a malware's execution
6	The Sandbox solution have File Type supported should included the following:
	.BAT, .BZ2, .CHM, .DLL, .eml, .exe, .GZ, .iso, .JAR, .JS, .JSE, .LNK, .MSI, .MHTML
	Microsoft Office Documents, including .DOC, .DOCX, .MSG, .RTF, .XLS, .XLSX, .PPT, .PPTX
	.PDF, .PE32, .PS1, .SEP, .SLK, .SWF, .TAR, .VBE, .VBN, .VBS, .WSF, .XML
7	The Proposed sandbox solution must have minimally support for Win7, Win 10 (x32, x64) or more
	The Proposed sandbox solution must concurrently support 50 or more VMs
8	The Sandbox solution must Support of analysis of file size of up to 100MB
9	The Sandbox solution must Support of URL analysis
10	The proposed sandbox solution should be able to track for network I/O to raw disks and any modification to MBR made by the samples during the dynamic analysis
11	The proposed sandbox solution should allow user to manually interact with the sample within the analysis environment while the analysis is taking place
12	The sandboxing capability of the proposed solution must be resistant to evasion techniques and report such behaviors if seen
13	Reports from the proposed malware analytics/Sandbox system must be organised in an easily understood manner so that first responders can comprehend and reduce need for security expertise to interpret reports
14	A video recording of the malware analysis should be made and be able to have playback and download capability for further analysis. security expertise to interpret reports
15	The sandbox solution should be appliance based with the ability to run multiple versions of Windows within the same environment
16	The Sandbox solution should be a proprietary custom built malware analysis solution and not open source or generic sandbox
17	The Sandbox solution shall be able to detect memory residing malware

18	The sandbox solution must provide safe and highly secure on-premises static and dynamic malware analysis to maintain the confidentiality of data.
19	The sandbox solution must have a user interaction tool that provides a safe environment to dissect malware without the risk of infecting customer network. Built into the appliance, analysts are able to interact with the sample while it is being analyzed including opening applications, clicking through dialogue boxes, and even reboot the virtual machine if needed
20	The sandbox solution must have comprehensive security insight into malware behavior and direct links to the sample source and associated behavior in sandbox extensive database
21	The sandbox must Provides easy access to all information and analysis results for further investigation
22	The sandbox must have capability to Analyze more than 800+ highly accurate and actionable advanced behavioral indicators
23	The sandbox solution must capability for automatically derives threat scores from proprietary analysis and algorithms that consider the confidence and severity of observed actions, historical data, frequency, and clustering indicators and samples. Prioritizes threats with confidence to reflect each sample's level of malicious behavior. Improves the prioritization of threats, which enhances the efficiency and accuracy of malware analysts, incident responders, security engineering teams, and products that consume sandbox feeds
24	The sandbox solution must have capability to be manually updated to help ensure an up-to-date knowledge base while complying with customer or regulatory policies to keep all information within logical boundaries
25	The sandbox solution must integration and easy with sandbox representational state transfer (REST) API & provides integration for a number of third-party products, including gateways, proxies, and security information and event management (SIEM) platforms
26	The sandbox solution must supports easy-to-integrate normalized feeds in a number of standardized formats - including JavaScript Object Notation (JSON), Structured Threat Information Expression (STIX), and comma-separated values (CSV) - and as Snort rules
27	Proposed Sandbox solution must support 2 x 10G interface and redundant power supply from day one
28	Proposed Sandbox solution must support Advance Analysis of 1500 sample per day

(Email Security)

Technical Requirement: Email Security Gateway Specification:		
S.No	**Feature**	**Minimum Requirement Specification**
1	**Platform Requirement**	The email security system offering should be dedicated OEM Appliance based solution and not a subset of NGFW, Proxy or other security solution
2		The gateway should support a comprehensive email security solution that integrates inbound and outbound defenses against latest email threats such as Spam, viruses, Malicious URL Blocking, URL category based filtering, safe unsubscribing, Robust anti-APT, DNS RBL verification, reputation filtering, DLP, and Encryptions utilizing a strong global threat intelligence capability
3		The solution should support 1**,500** users for anti-spam, anti-virus, virus outbreak, data loss prevention and encryptios, Anti-APT, , phishing etc and scalable to 3000 in future. All features required from day one.
4		Solution must offer complete defense against email threats with 99%+ anti-spam accuracy
5		Solution should have false positive efficacy of 1 in 1 million
		To improve spam efficacy solution should derive verdict based on IP Address, infrastructure provide, fully qualified domain name and other sender information in SMTP conversation
		Solution should support capability to securely send messages to valid recipient domain by enabling DNS-based authentication of name entities for outgoing TLS connections
6		Propose solution should not be software based and installed in mail server. It should be purpose built dedicated email security gateway.
7	**MTA Appliance Features**	The solution should use their own operating system and MTA on appliance and not open source based operating system , i.e Qmail, Sendmail etc. MTA system should be purpose built and optimized for Messaging Queuing which should maintain separate queues for each destination domain to avoid single queue issues
8		The MTA should be able to send multiple messages per connection and be able to open multiple connections per host and should support RFC 2821 compliant Simple Mail Transfer Protocol (SMTP) to accept and deliver messages
9		The solution should support ability to perform SMTP session control and traffic rate limiting according to sender's IP address/range, domain or email reputation. The solution should be able to assign maximum SMTP sessions per IP address on appliance
10		The solution should perform SMTP conversational bounce for invalid recipients (prevent Non-Delivery Report Attack), directory harvest prevention, and have ability to perform SMTP session control and traffic rate limiting (down to per recipient) according to sender's IP address/range, domain or email reputation.
11		Solution should have Multi-layer Anti-spam filter: It should have capability to scan mails for spam with 3rd party SPAM engine before OEM Spam engine.
12		The solution should have anti-virus scanning available within the appliance
13		The solution should provide protection against zero-day and targeted attacks. It should be able to dynamically analyze message attachments for malware without sending files to cloud

14		The proposed solution should include Anti-APT / Next Generation detection ability to quarantine emails suspected to been infected with malware both for inbound as well as outbound email
15		The proposed solution shall support the ability to hold the email until sandbox analysis is complete and the threshold shall be configurable
		The proposed sandbox appliance should support 50 or more virtual machines running simultaneously and should have integrated redundant power supply along with capability to support 10G interface
		To proactively respond to cyber threats such as malware, ransomware, phishing attacks, solution should have capability to consume external threat information in STIX/TAXII
16		The solution should provide virus outbreak prevention on abnormal increase of emails with specific email attachments
		Solution should support scanning of URLs in message attachment and perform action on such message.
17		The solution should provide the URL defense service to: Re-write the original suspicious URL in the mail body to another URL and On clicking the re-written URL, the browser session should pass through a cloud based Web security scanning infrastructure of the same OEM
		Solution should be able perform URL filtering on shortened URIs, and retrieve actual URL from shortened URL and perform action on the basis of reputation score
18		The solution should provide capability of the appliance to perform recipient validation by querying an external SMTP server prior to accepting incoming mail for the recipient
19		Solution should provide forged email detection protection against business executive compromise and provide detail logs on all attempts and actions.
20		The solution should support policies to sign outgoing emails based on domain key and allow to sign by different domain keys based on sender domain
21		The solution should support outbound SMTP over TLS based on destination domains or system wide and support outbound SMTP authentication
22		certificate management capabilities for S/MIME encryption and/or digital signatures including supportforaccess to public key repositories, ability to harvest public keys from received emails, and export/import of public keys both individually or inbulk.
23		Support to selectively apply digital signatures on outbound emails including capability to apply digital signatures based on policy using mail or other attributes.
24		Support for adding DKIM signatures on outbound email including the capability to selectively apply DKIM signatures based on policy and apply different DKIM signatures based on policy or domain.
25		Support for SPF, DKIM, and DMARC email authentication including ability to apply email authentication requirements based on domain (specific or wildcard), ability to quarantine emails failing authentication,DMARC reporting,and any other authentication policy features.Include ability toselectivelyconfirm email authentication success (SPF, DKIM, DMARC) for inbound messages on other filtering policies that may include whitelisting of those addresses.
26		Appliance should have DLP feature so that organization can deploy DLP as per their compliance and require database

27		Support Multi-layer Anti-spam filter: TCP connection level Reputation Filtering (Sender IP/domain) On Box Anti-spam Filtering Allow integrated use of different vendor anti-spam engine The spam rules should be automatically updated every 5 minutes Solution should be able to distinguish between spam and marketing mail from a legitimate source
28		The solution should support following for system monitoring: - SNMP v2/v3, MIB-II, XML, Syslog support
29		The solution should support authenticate users using RADIUS or LDAP and two-factor authentication for secure access into appliance for management purpose
30		The appliance should support the use of IPv6 for: o Appliance interfaces o Gateways (default routes) o Static routes o SMTP Routes o Querying external SMTP server with IPv6 address (for Recipient validation) o IPv6 Sending hosts o Content Filters o Sending to IPv6 destinations o Report searches
31	Warranty and support	Support should be directly from OEM through India based TAC center and should support 24x7.

(Router Internet GW)

	Network Router (Internet Gateway) with Power Redundancy
1	The Router should support modular architecture, multi-core (more than 2) Processor. Router should have 1:1 redundant internal field replaceable power supply (from Day1).
2	Router should have 6 x 1G SFP WAN ports and 2x10G SFP WAN Ports, Bidder to provide 6x1G SX SFP and 2x10G SR SFP+ from Day-1
3	The Router should support interfaces like Channelized E1/T1, Channelized STM-1, STM-4, STM-16, E3/T3, Serial V.35, G.703, Gigabit and 10G Ethernet modules. All the modular interfaces on the router should support hot-swapability feature to accommodate field upgrades without rebooting the router.
4	The Router should have at least one empty slot for future use
5	Router should have minimum 8 GB of DRAM/SDRAM and 1GB Flash from Day 1 and upgradeable to 16GB DRAM.
6	The router must support IKEv1, IKEv2, GRE and IPSEC from day 1. The proposed solution should serve the GRE encryption for traffic from any location to other location on demand and also should able to create GRE tunnel.
7	Routers should support 20 Gbps WAN throughput from day1
8	Router should support 1000K IPv4 / IPv6 routes
9	Router should support 4000 GRE / IPSEC tunnel.
10	The router should have support 4000 Mbps of IPSEC Bandwidth
11	Router should support IGMP v1/v2/v3, PIM multicast routing and IPv6 Multicast
12	Router should support static Routes, OSPFv2, OSPFv3, BGP4, MBGP, BFD, Policy based routing, IPv4 and IPv6 tunneling, MPLS from Day 1
13	The Router should support Zone Based Firewall feature
14	Router should Support Traffic Optimization feature built in the router operating system or an external appliance for the same functionality can be provided.
15	Router shall support of QoS and Up to 16,000 queues

16	Router should support NAT
17	The router must support router redundancy protocol
18	Should have extensive support for IP SLA or equivalent and best path selection for metrics like delay, latency, jitter, packet loss to assure business-critical IP applications from Day1.
19	Router shall conform to UL 60950 or IEC 60950 or CSA 60950 or EN 60950 Standards for Safety requirements of Information Technology Equipment.
20	Router should be tested and certified for EAL 3/NDPP or above under Common Criteria Certification
21	Router should be IPv6 Certified/IPv6 logo ready
	Switch should be of an OEM who is a Gartner leader in Wired and Wireless Infrastructure or DC Networking

(Router WAN Aggregation)

	Network Router (WAN Aggregation) with Power Redundancy
1	The Router should support modular architecture, multi-core Processor (more than 2). Router should have 1:1 redundant internal field replaceable power supply (from Day1).
2	Router should have 4 x 1G WAN ports, out of which 4 ports can be 1G SFP or 10/100/1000 BaseT port from Day-1. Bidder to provide 2 number 1G SX SFP from day-1. Router Should be upgradeable to additional 6x1G Combo WAN ports in future
3	The Router should support interfaces like Channelized E1/T1, Serial V.35, G.703, Gigabit and 10G Ethernet modules. All the modular interfaces on the router should support hot-swapability feature to accommodate field upgrades without rebooting the router.
4	The Router should have at least Three empty slot for future use
5	Router should have minimum 4 GB of DRAM/SDRAM and 2GB Flash from Day 1. .
6	The router must support IKEv1, L2TP, IKEv2, GRE and IPSEC from day 1. The proposed solution should serve the GRE encryption for traffic from any location to other location on demand and also should able to create GRE tunnel.
7	Routers should support 1 Gbps WAN throughput from day1 and should support upgradable to upto 4 GBPS
8	Router should support 500K IPv4 / IPv6 routes, with 2000 GRE / IPSEC tunnel.
9	The router should have 400 Mbps of IPSEC Bandwidth and should support 800 Mbps IPSEC Bandwidth incase required in the future
10	Router should support IGMP v1/v2/v3 and PIM multicast routing
11	Router should support static Routes, OSPFv2, OSPFv3, BGP4, MBGP, BFD, Policy based routing, IPv4 and IPv6 tunneling from Day 1
12	The Router should support Zone Based Firewall feature or an external appliance for the same functionality can be provided.
13	Router should Support Traffic Optimization feature built in the router operating system or an external appliance for the same functionality can be provided.
14	Router shall support of QoS
15	The router must support router redundancy protocol
16	Should have extensive support for IP SLA or equivalent and best path selection for metrics like delay, latency, jitter, packet loss to assure business-critical IP applications from Day1.
17	Router shall conform to UL 60950 or IEC 60950 or CSA 60950 or EN 60950 Standards for Safety requirements of Information Technology Equipment.
18	Router should be tested and certified for EAL 3/NDPP or above under Common Criteria Certification
19	Router should be IPv6 Certified/IPv6 logo ready
20	Switch should be of an OEM who is a Gartner leader in Wired and Wireless Infrastructure or DC Networking

Core Switch (Layer -3)

Sr. No.	Feature Set
1	**Solution Requirement**
1.1	The Switch should support non-blocking architecture, wire speed line rate performance
1.2	The switch quoted should be part of latest Gartner's Leader Quadrant for Data Center networking. All the switches should be from same OEM

2	**Hardware and Interface Requirement**
2.1	Switch should have the following interfaces: 48 x 1G/10G and 6 x 100G ports populaated with Fiber Interface 24x10G multi mode and 24x1G multi mode interfaces
2.2	Switch should have console port
2.3	Switch should have management interface for Out of Band Management
2.4	Switch should have a minimum 40MB buffer of more.
3	**Performance Requirement**
3.1	Switch should support minimum 512 VRF instances
3.2	The switch should support hardware-based load balancing at wire speed using LACP and multi chassis EtherChannel/ LAG EtherChannel/ LAG
3.3	Switch should support minimum 3.6 Tbps of non blocking Switching bandwidth
4	**Virtualization Features**
4.1	Switch should support Network Virtualization using Virtual Over Lay Network using VXLAN (RFC 7348)/NVGRE as per RFC 2890
4.2	Switch should support VXLAN (RFC7348) and EVPN for supporting Spine - Leaf architecture to optimise the east - west traffic flow inside the data center
4.3	Switch should support Open Flow/Open Day light/Open Stack controller
5	**Layer2 Features**
5.1	Switch should support VLAN Trunking (802.1q) and should support 3000 VLAN
5.2	Switch should support minimum 64K no. of MAC addresses
5.4	Switch platform should support MACSec in hardware
6	**Layer3 Features**
6.1	Switch should support static routing, OSPFv2, OSPFv3, ISIS, BGPv4, MP-BGP, EVPN
6.2	Switch should provide multicast routing like PIM, MSDP
7	**Availability**
7.1	Switch should have provisioning for connecting to 1:1/N+1 power supply for usage and redundancy
7.2	Switch should provide gateway level of redundancy in IPv4 and IPv6 using HSRP/VRRP
7.3	Switch should support for BFD For Fast Failure Detection
8	**Quality of Service**
8.1	Switch system should support 802.1P classification and marking,
9	**Security**
9.1	Switch should support control plane i.e. processor and memory protection from unnecessary or DoS traffic by control plane protection policy
9.2	Switch should support for external database for AAA using: TACACS+ and RADIUS
10	**Manageability**
10.1	Switch should support for sending logs to multiple centralized syslog server for monitoring and audit trail
10.2	Switch should provide remote login for administration using: Telnet, SSHv2
10.3	Switch should support for basic administrative tools like PING, TRACEROUTE
10.4	Switch should support central time server synchronization using Network Time Protocol NTP v4
10.5	Switch should provide different privilege for login in to the system for monitoring and management
11.2	Switch and optics should be from the same OEM

(Edge Switch Layer -2)

1.1	**Edge Switch - 24 Port (Non-PoE)**
1.2	**Generic Requirements**
1.3	Switch should be 1RU with minimum 24 nos. 10/100/1000 Base-T ports and additional 4 nos. SFP+ uplinks ports. Switch should be loaded with 4 no. of 10G SRModule from Day1." As per requirement
1.4	Switch should have slot/ports (excluding uplinks) for minimum 80 Gbps of stacking bandwidth with dedicated stacking ports and cables with minimum 8 switch in stack.

1.5	Switch should support internal field replaceable redundant power supply. Switch should support redundant fans.
1.6	Switch shall have minimum 128 Gbps of switching bandwidth and 95 Mpps of forwarding rate.
1.7	Shall have minimum 16K MAC Addresses and 1024 active Vlans.
2	Switch should support for L3 functionality like static routing, RIP, PIM, OSPF, PBR ,MACSec-128, & QoS features from Day1
2.2	Should support 802.1x authentication and accounting, IPv4 and IPv6 ACLs
2.3	Should support 3000 IPV4 & 1000 IPV6 routing entries and 1000 multicast routes
2.4	Switch shall support application visibility and traffic monitoring with minimum 12 K netFlow/sflow/jflow entries.
2.5	The switch should support Jumbo frames of 9000 bytes
2.6	should have 2 GB RAM and 1 GB Flash
4	**Certifications and Environment**
4.1	Switch should be of an OEM who is a Gartner leader in Wired and Wireless /DC networking Infrastructure
4.2	Safety certifications - IEC 60950-1 / UL 60950-1 / EN 60950-1,
4.3	Electromagnetic emissions certifications - Class A or better EN 300 386 EN61000-3-2 EN61000-3-3 EN 55032:2015 Class A, EN55024
4.4	Environmental - Reduction of Hazardous Substances (ROHS) 5 and above
4.5	Normal operating temperature : 0ºC to +45ºC
4.6	Switch should be tested and certified for EAL 2/NDPP or above under Common Criteria Certification.
5	**Operation**
5.1	· WebUI: Should support WebUI to be used as an embedded GUI-based device-management tool that provides the ability to provision the device, to simplify device deployment and manageability
5.2	5 Years onsite OEM Warranty

For SLB/ADC

Technical Specifications
OEM Eligibility Criteria
The proposed Load Balancer should be listed in latest Gartner's Market Guide for ADC and should be among the Top 5 Vendors according to the latest IDC Report for ADC.
Architecture
Traffic ports supported: 4 X 10G SFP+ and 4 x 1G ports 1 X 1G RJ 45 Management Port Layer 4 CPS: 500,000, Layer 7 RPS: 500,000 RAM: 64 GB, HDD: 4 TB

Should provide minimum 5 Gbps throughput and can be scalable to 20 Gbps throughput without changing the hardware (license upgrade only).
Device must have Dynamic routing protocols like OSPF, RIP1, RIP2, BGP from Day 1
Following Server Load Balancing Topologies should be supported: ○ Virtual Matrix Architecture / Equivalent ○ Client Network Address Translation (Proxy IP) ○ Mapping Ports ○ Direct Server Return ○ One Arm Topology Application ○ Direct Access Mode ○ Assigning Multiple IP Addresses ○ Immediate and Delayed Binding ○ IP Address Ranges Using imask / Equivalent
Load Balancing Features
The SLB should support the below metrics: a) Hash b) Persistent Hash c) Least Connections d) Round Robin e) Response Time f) Bandwidth g) SNMP
VIRTUALIZATION: The proposed SLB should have ADC-VX/Virtualization feature that virtualizes the Device resources—including CPU, memory, network, and acceleration resources. a) Resources b) Configurations c) Management d) OS The proposed device should support up to 8 Virtual Instances including the capability to install and run third-party and open source software on the same appliance from Day 1
The SLB should support Role based Access for Administration and the Appliance should be ICSA Certified (System or any supported component) The solution should have license upgrade feature on same appliance to support machine authentication based on combination of HDD ID, CPU info and OS related parameters i.e. mac address to provide secure access/authentication to corporate resources.
The device should support DNS SEC Global Server load Balancing functionality. It should be capable of handling complete Full DNS bind records including A,MX, AAAA, CNAME, PTR, SOA etc..

A framework for customizing application delivery should be provided using user-written scripts that provides the flexibility to control application flows and fully meet business requirements in a fast and agile manner. The proposed framework should enables to: o Extend Server Load Balancer Fabric services with delivery of new applications
○ Quickly deploy new services ○ Mitigate application problems without changing the application ○ Preserve infrastructure investment by adding new capabilities without additional equipment investment
Should support Web Performance Optimization feature that should employ different acceleration treatments for different application and browser scenarios: ○ Simplifying large, complex web pages. ○ Caching ○ Accelerate entire web transaction ○ Third-Party timing and SLAs ○ Content Magnification / Equivalent ○ Acceleration for mobile devices--Mobile Caching, Image resizing, Touch-to- click conversion / Equivalent
DNSSEC based Global Load Balancing should be supported in the proposed device.
1) The Solution should include Monitoring and Reporting System which shall support custom reports such as "Top Response Codes", "Top Error Codes" and other dashboards with support for filtering/customizing reports
Should support server side web compression and proximity based LLB. The Appliance should also support acting as a Web agent service to implement explicit Forward proxy mode and to perform DNS Caching
Redundancy
Should Support standard VRRP (RFC - 2338)
SLB Device should be accessed through the below: ○ Using the CLI using SSH and Telnet Using SNMP ○ REST API ○ Using the Web Based Management ○ Dedicated Management Port

WAF- (specification should be include in ADC solution no Separate Hardware required)

OEM ELIGIBILITY CRITERIA
The proposed WAF module should be ICSA certified.
Architecture
The Proposed WAF Module should be a part of Next-Generation, Multi-Tenanted Platform capable of installing and running third-party and open source software on the same appliance from Day 1. The Appliance should have minimum 64 GB RAM and 4 TB HDD.
Should have WAF throughput of 1.5 Gbps

Traffic ports supported: Inbuilt with SLB/ADC
The proposed device should have ADC-VX/Virtualization feature that virtualizes the Device resources—including CPU, memory, network, and acceleration resources. Each virtual instance contains a complete and separated environment of the Following: a. Resources b. Configurations, c. Management, d. OS The Proposed device should support up to 8 Virtual Instances including the capability to install and run third-party and open source software on the same appliance.
WAF should have the flexibility to be deployed in the following modes:
a. Reverse proxy
b. Transparent Proxy c. Forensic (Offline) Mode
The proposed solution should support standard VRRP (RFC - 2338) for High Availability purpose (no proprietary protocol).
The WAF Module should have the ability to work with: a. Raw Traffic b. Mirrored Traffic c. PCAP Files d. Web Server Log Files
The Solution must be able to protect against (but not limited to) OWASP Top 10 Attacks from Day 1
Hiding Sensitive Content Parameters: It should be able to Mask values of sensitive parameters (for example, passwords, credit card and social security details)
WAF should support for IPv4 and IPv6 traffic
The proposed solution should also be able to detect attacks using retrospective analysis of webserver access logs to investigate, previously occurred events (historical events in past before deployment of WAF or to detect attacks in applications not protected by WAF)
proposed solution should include a passive vulnerability scanning engine with ability to detect suspicious requests and compromise responses of the applications. For example, based on a malicious sql query from the user and based on the application response, the passive vulnerability scanner should be capable to detect application vulnerability that is being exploited or attempted to be exploited.
Management capabilities including but not limited to: Dashboard management: • Sorting by any of the displayed event attributes • Filtering by any of the displayed event attributes or their combination • Lucene query syntax support for sophisticated filters • Multi-level aggregation (grouping of the events with the same values of attribute) Correlation • Correlations and attacks chains that allow to group related events (including specifying the exact order of their occurrence) and to identify complex attacks using predefined and custom rules • Correlation engine should have the capability to define and detect custom user specified events and combine these events into one correlation event. For example, the proposed solution should detect SQLi Probing event, SQLi Number Guessing event, SQLi Data extraction or Data injection event. Furthermore, these multiple events should can be added into one correlated event, to provide user defined attack chains that can alert the user of a specific defined attack.

• Correlation engine should have ability of compromise detection based on application responses, if the WAF is configured on detection mode. For example, detect successful exploitation of XSS based on application response to a malicious request.
The Proposed WAF Module should support the following Security Features: a. The proposed solution should integrate with Source code analysis solution that can identify vulnerabilities in technologies like Java, PHP, C# VB.Net, Python, C/C++. The proposed silution should provide report based integration with the mentioned source code analysis solution to gain information on the vulnerability entry point, control flow and data flow of the vulnerable function. b. The proposed solution should be able to automatically build data model for unlimited number of attribute in HTTP request (e.g. parameters, headers, cookies) using a known and established Machine Learning technology to identify anomalous traffic going to the protected application. This Machine learning modeling should be completely executed Unassisted, and should not just build data models, but also detect changes to application attributes and retrain the built data models automatically. c. The proposed solution should also be able to detect attacks using retrospective analysis of webserver access logs to investigate, previously occurred events (historical events in past before deployment of WAF or to detect attacks in applications not protected by WAF)
The solution must support integration with third party DAST and SAST tools to perform virtual patching for its protected web applications. The solution must support proposed web application vulnerability assessment tolls to virtually patch web application vulnerabilities.
The WAF should use a Intelligent Detection advanced machine learning technology for identifying web attacks and minimizing false positives/negatives and deliver next-gen real-time web security. The auto-learning should function on production traffic and learn all application parameters and should be able to create policies based on those parameters as well.
The proposed solution should provide a flexible dashboard and provide at a minimum provide the following information. Additionally, the dashboard should be used to generate statistical and graphical information (Charts, bar graphs, tables) for analysis purposes, to enable quick analysis on the dashboard itself. • Source of attack: • IP address and TCP port, • Geolocation, • OS name and version, • Browser name and version, • Full list of request parameters, headers and their values, • Username (if any), • Request body • Target of attack: • Protected application ID, • URI, • Full list of response headers and their values; • Response code, • Response body, • Time of response • Event: • Unique Event ID, • Event priority, • ID of protector that detected the attack, • Attack description, • Carrier of the attack payload (request or response attribute), • List of actions performed to mitigate the attack

The dashboard should also have grouping capabilities to represent the same information, in multiple possible combinations. For e.g. Matched event tags can be grouped further by Client Source Country or IP etc.

	Privileged Access / Identities Management
1	All privileged access management operations and communications must adhere to maximum security standards and best industry practices. The proposed solution should not pose a security or operational risk to the Entire Infrastructure and application.
2	Must implement granular privileged access policies and enforce these policies on Entire Infrastructure and application systems from a single management platform independent of Microsoft Active Directory, local Linux security sub systems and other local authentication and authorization systems
3	Must interoperate with the SIEM solution to store its logs and other operational data for extended period of time.
4	Must natively integrate and interoperate with all ƒ Operating Systems, Virtualization, and Containers: Windows, *NIX,IBM iSeries, Z/OS, OVMS, ESX/ESXi, XenServers, HP Tandem*,MAC OSX*, Docker
4.1	Windows Applications: Service accounts including SQL server service accounts in cluster, Scheduled Tasks, IIS Application Pools, COM+, IIS Anonymous Access, Cluster Service
4.2	ƒ Databases: Oracle, MSSQL, DB2,Informix, Sybase, MySQL and anyODBC compliant database
4.3	Security Appliances: CheckPoint,Cisco, IBM, RSA Authentication Manager, Juniper, Blue Coat*,TippingPoint*, SourceFire*, Fortinet*, WatchGuard*, IndustrialDefender*, Acme Packet*, Critical Path*, Symantec*, Palo Alto*
4.4	Network Devices: Cisco, Juniper*, Nortel*, HP*, 3com*, F5*, Nokia*,Alcatel*, Quintum*, Brocade*, Voltaire*, RuggedCom*, Avaya*,BlueCoat*, Radware*, Yamaha*McAfee NSM*
4.5	ƒ Applications: CyberArk, SAP, WebSphere, WebLogic, JBOSS, Tomcat, Cisco, Oracle ERP*,Peoplesoft*, TIBCO*
4.6	Directories: Microsoft, Oracle Sun, Novell, UNIX vendors, CA
4.7	Remote Control and Monitoring: IBM, HP iLO, Sun, Dell DRAC, Digi*, Cyclades*, Fijitsu* and ESX
4.8	Configuration files (flat, INI, XML)
4.9	Public Cloud Environments: Amazon Web Services (AWS), Microsoft Azure, Google Cloud Platform (GCP)
5	The proposed PAM solution must be extensible and scalable to accommodate the college's growing needs and keep up with complex operational requirements
6	Must support on premises and cloud based multi factor authentication solutions.
7	Must offer capability to grant audited temporary access to critical college systems in case of an emergency access required (Break Glass Procedure).
8	Must provide extensive analytics, reporting and notification functionality to alert college staff about suspicious activities.
9	Provide detailed activity auditing for privileged accounts, including service and shared/generic accounts
10	Provide capability to log and record clicks, keystrokes and commands associated with a privileged account and provide a detailed audit log that shows these activities clearly when it is needed.
11	Encryption Algorithms:AES-256, RSA-2048 ,HSM integration, FIPS 140-2 validated cryptography
12	Ability to manage credentials for privileged, shared, generic, application and service accounts.
13	Must support password checkout with configurable timeouts and automatic password randomization and able to reset them after use
14	Ability to perform sequential screen capture and full video recording.

15	Ability to build workflows that support both manual and automatic approvals.
16	Facilitate enforcements of PCI, FERPA, HIPPA compliance and reporting.
17	Seamless Integration with the existing and planned security systems and tools.

Virtualization Hypervisor & Management Cosnole	
1	Should Support 1-4 CPU Sockets of Intel and AMD
2	Provide a purpose-built hypervisor with minimal footprint that installs directly on the bare metal x86 server hardware with no dependence on a general purpose OS for greater reliability and security.
3	Provide a highly-available administrative console for management of the virtual data centre platform to conduct activities such as onboarding/managing/updating hosts, virtual machines, storage and networks.
4	Provide the ability to create new virtual machines from scratch or based on templates (created from fully configured virtual machines)
5	Provide the ability to boot from iSCSI, FCoE, Fibre Channel SAN , locally attached USB storage and network PXE boot.
6	Provide support for heterogeneous guest operating systems such as Windows (Desktop & Server OS) and Linux (at least Red Hat, SUSE, Ubuntu and CentOS) and Solaris x86.
7	Provide a built-in convertor to migrate physical Windows and Linux workloads to virtual workloads
8	Provide automated live migrations for initial placement and balancing of available resources with rules to define affinity and/or anti-affinity for workloads (eg. 2 VMs providing availability for each other should always be placed on different hosts).
9	Provide the ability to hot-add cpu and memory and hot-plug disks and NICs (provided the same is supported by the guest operating system).
10	Provide the ability to expand virtual disks (boot and non-boot disks) without downtime and provide options for locating new virtual disks for existing workloads on different tiers of storage for both Windows and Linux workloads.
11	Provide I/O prioritization for virtual workloads to ensure that business critical VMs are not affected due to congestion by other VMs on the same host.
12	Provide a highly-available platform with built-in clustering capability leveraging both network & storage communication for cluster heartbeats. Failure of the management network shall not result in downtime for the workloads
13	Provide zero downtime hosts patching with maintenance mode to move running workloads to other hosts on the platform with a consistent audit trail of the patching process.
14	Support configurations of 802.1q VLANs which are compatible with standard VLAN implementations from other vendors.
15	Support an option to securely boot workloads using the UEFI (Unified Extensible Firmware Interface) when available in hardware to ensure that only signed drivers & OS loaders are loaded while booting
16	Support AES-128 and AES-256 encryption (in conjunction with any KMIP 1.1 compliant KMS server) of the workloads when at rest on storage without modifying the Guest OS.
	Management Console
1	Virtualization management software console should provide a single view of all virtual machines, allow monitoring of system availability and performance and automated notifications with email alerts.

2	The virtualization management software should provide the core administration interface as a single Web based interface. This interface should be flexible and robust and should simplify the hypervisor control through shortcut navigation, custom tagging, enhanced scalability, and the ability to manage from anywhere with Internet Explorer or Firefox-enabled devices.
3	The management software should provide means to perform quick, asneeded deployment of additional hypervisor hosts. This automatic deployment should be able to push out update images, eliminating patching and the need to schedule patch windows
4	Virtualization management software console should provide reports for performance and utilization of Virtual Machines. It shall co-exist and integrate with leading systems management vendors
5	Virtualization management software console should allow to Move a powered off virtual machine from one physical server to another by dragging and dropping the virtual machine icon and allow cloning of both powered on and powered off virtual machines.
6	Virtualization management software console should maintain a record of significant configuration changes and the administrator who initiated them.
7	Virtualization management software console should provide the Manageability of the complete inventory of virtual machines, and physical servers with greater visibility into object relationships.
8	Virtualization management software should provide a global search function to access the entire inventory of multiple instances of virtualization management server, including virtual machines, hosts, data stores and networks, anywhere from within Virtualization management server
9	Virtualization management software should support user role and permission assignment (RBAC).
10	Virtualization management software should allow you to deploy and export virtual machines, virtual appliances in Open Virtual Machine Format (OVF).
11	The management solution for hypervisor should provide Single-Sign-On capability which should dramatically simplify administration by allowing users to log in once to access all instances or layers of management without the need for further authentication.
12	The management solution should provide alerts with symptoms and recommended actions for known problems with the ability add custom alerts (with symptoms and recommended actions).
13	The management solution should be able to collect and analyze all types of machine-generated log data, for example, application logs, network traces, configuration files, messages, performance data and system state dumps.

NMS	
1	**Core Monitoring Capabilities**
a	The proposed monitoring solution should be able to monitor: (a) Routers (b) Switches (c) Firewalls (d) devices (e)Servers (f) Other SNMP-enabled devices(g)Database (h) Middlwaware and other applications (i) URL (j) Ports upto 100 Devices
b	Should automatically provide real-time, in-depth network performance statistics after discovery/configuration of devices, including but not limited to, (a) CPU load (b) Memory utilization (c) Interface utilization (d) packet loss
c	Should show statistics like interface bandwidth, current traffic in bps, total bytes received/transmitted etc.
d	Should display information including alerting for major, routing protocols (BGP, OSPF , RIP, EIGRP) with options to view and search routing tables including VRFs, changes in default routes and flapping routes, router topology and neighbor statuses

e	Should help with multicast traffic information monitoring, alerting including topology information, multicast information, route information, multicast errors etc.
f	Should display device status and interface status by different colors to represent warning and critical status
g	Should show both real time details and historical details in form of charts with option to choose the time periods
h	Should monitor hardware health for popular vendors and should allow alerting and reporting on hardware health monitoring
i	Should have options to poll using SNMPv3 and WMI, with complete encryption methodology, Only those devices where SNMP v3 is not available, the SNMP v1 or 2 can be considered.
j	Should have options to configure polling intervals as needed
k	Should have options to specify data retention periods
2	**Network Discovery**
a	The proposed monitoring solution should be able to discover devices in the network with SNMP and ICMP capabilities automatically, on input of, (a) IP address ranges (b) subnets (c) individual IP addresses
b	Should have option to automate and schedule discovery process
c	Should prompt in web console on discovery of new devices in network
d	Should use discovered information for creating topology maps
3	**Graphical User Interface and Customization**
a	The proposed management solution should provide a high-quality graphical user interface with asynchronous view refreshing
b	This web console should be accessible centrally or remotely
c	The web console should allow multiple users to log in at the same time
d	It should provide a unified view of alerts, traps, events, syslog messages in a single page
e	It should quickly highlight devices with issues, based on different properties like response time, cpu load, memory usage, high interface usage etc.
i	It should allow creation of custom dashboards and restrict views for users based on devices or interfaces, i.e. it should have role-based access
g	It should log user actions and events in the web console for audit purposes and they should be available for alerting and reporting
h	It should allow export of any web page in console to PDF format
i	It should integrate with Active Directory for user login purposes
4	**Advanced Reporting**
a	The proposed monitoring solution should provide current and historical out-of-the-box reports for various statistics monitored
b	Should be able to generate / create the report via the web console
c	Should be able to generate statistical reports that can be used as reference for future planning or troubleshooting
d	Should allow customization of reports by adding/removing columns, setting filters, specifying timeframes, grouping columns etc.

e	Should allow reports to be sent out on schedule as daily, weekly, monthly reports
f	Should allow emailing of dashboards created in web console
g	Should be able to configure both charts and tables into a single report.
h	Should have options to import/exports reported created by other users
	Should support multiple formats such as pdf, HTML and CSV
5	**Advanced Alerting**
a	The proposed monitoring solution should be able to manage and display events/alerts in the web console
b	The alerts and events information should be logged into the database for future reference
c	It should allow creation of new alerts from scratch and also customizable threshold limits
d	It should allow creation of alerts based on sustained states
e	Should have various actions that can be taken, including but not limited to, sending out emails, forwarding SNMP traps, running executables, sending SMS textalerts, playing sound, emailing a web page etc.
f	Should have the ability to dynamically baseline statistics and automatically set Warning and Critical threshold
6	**Grouping**
a	The proposed monitoring solution should allow grouping of devices by various properties -- by department, by location, by name and by other properties gathered
b	Should also allow adding members to groups on-the-fly by specifying a property which can dynamically change values, like volumes reaching low free space
c	Should be able to define dependencies and relationships between connected devices and interfaces to avoid false-positive email alerts in case of outage.
7	**Network Maps**
a	The proposed monitoring solution should be able to represent the network pictorially and display performance details of devices in real time
b	Should allow customization of background, icons etc. and should allow multiple network maps to be nested with drill-down capabilities
c	Should be able to display not just the device status on the map but also status of any other detail obtained through custom MIB polling
d	Should be able to automatically connect devices by means of topology information gathered during discovery, like Cisco Discovery Protocol or Link Layer Discovery Protocol
e	Should be able to view multicast topology using upstream and downstream device list information
f	Should have the ability to show the link utilization
8	**Multi-vendor Support**
a	The proposed monitoring solution should not be vendor-specific
b	The discovered devices should be detected as that of a specific vendor and categorized automatically
9	**Application Aware Network Performance Monitoring**
a	Should be able to provide Network Response Time (NRT) and Application Response time (ART) for critical applications
b	Should have the ability to create custom HTTP applications
c	Should be able to contextually provide QoE data for nodes in Node Details sub view

d	Should be able to monitor extensive properties of Webloigic , Database, Apache Tomcat and other applications etc
10	**Additional Components**
a	Should have utilities to view the database, to stop and start application services
b	Should have options to receive, display and alert on syslog messages and traps from devices
11	**Integration**
a	Should allow integration with third-party applications at user-interface layer, through message exchanges and also through APIs like service desk etc

Service Desk	
1	Solution includes integrated CMDB (Configuration Management Database) for managing key ITIL functions and processes: IT Service Desk, Incident, Problem, Change, Release, Configuration, Service Level.
2	Tool provides the ability to segregate tickets based on security and compliance requirements (HIPAA, FERPA, security incident information, etc.).
3	The solution supports ITSM process workflow between solutions users including routing of request, electronic request approvals by actionable e-mail, etc.
4	The solution supports ITIL Version 2 and Version 3 frameworks including terms and definitions
5	The solution supports a web-based client for user and administrative functions.
6	Ability of the solution to enable rapid deployment of new users and administration of existing users
7	Comprehensive permission control schema for administrator and management rights
8	Integrated satisfaction survey and reporting
9	User knowledgebase with smart search and self-resolution proposal
10	Integrated/automated self-help Internet search options with approved result management.
11	Automatic screen shot and asset service request attachment.
12	Conversation tree ticket tracking logs.
13	Chat messaging and email automatic request creation processes.
14	Task management with Parent/Child authoring requests and tracking.
15	Support up to 15 agents
16	Solution Should be fully customizable as per requirement

Annexure-5: Operations & Maintenance Activities

On-Site Operations & Maintenance Activities

Note: Please note that this list of O&M activities is indicative only and exhaustive. On-site O&M team shall carry out any additional activities as required by RailTel Customer for smooth operations and maintenance of its ICT Infrastructure.

The on-site O&M services shall include, but not limited to the following activities under scope -

1) **IT Help Desk:**

a) IT Help Desk shall act as a Primary point of contact for all events, incidents, service requests, and change requests received via telephone, emails, web interface (Help Desk), or automatically generated infrastructure events from NMS tools and infrastructure devices etc.

b) IT Help shall also perform Level-1 monitoring and alerting for fault, availability and performance of entire ICT infrastructure, log and escalate the incidents/issues/problem to concerned technical team for resolution.

c) All service request, incidents and change management shall be owned and maintained by Help Desk.

d) IT Help Desk shall support for logging calls related to ICT services/Infrastructure services, business applications, and facilities for Data Centre.

e) Primary responsibilities of IT Service desk shall include, but not limited to, the following:

i. Logging and Categorization of incidents, issues, service requests, and changes request related to ICT infrastructure under the scope of work and issue a Ticket ID number in the Help-desk tool.

ii. Assign severity level to each issue / incidents so as to maintain categorization and differentiate the criticality of the incident via the priority levels, severity levels and impact levels.

iii. Escalation issues/incidents/problem to internal and external entities, third-party vendors / concerned Service in-charge if necessary as per defined escalation matrix.

iv. Tracking each incident/service request to the resolution and Closing of incidents and service requests etc.

v. Provide feedback to the users.

vi. Analyze the issue / complaint statistics.

vii. Escalate the problems to the 3rd party Vendors / concerned Service in-charge if necessary as per defined escalation matrix, in coordination with technical teams.

viii. Creation of Knowledgebase, with the help of concerned technical teams on frequently asked questions (FAQ) to help users of ICT Infrastructure, as well on troubleshooting, diagnosis and known issues for incident and problem management.

2) **Hardware Maintenance**

a) Maintenance of all hardware components of RailTel Customer ICT Infrastructure including Servers (both existing as well as new supplied by the RailTel), Storages, Network and Security devices, tape libraries etc. in coordination with respective OEMs/vendors. Hardware support for the ICT infrastructure solution will include diagnosing the problem and resolving the problems in coordination with respective OEMs.

b) Periodic and regular upgrade of Server firmware and drivers, as and when released by OEM, in coordination with and as per OEM recommendations.

c) Preventive Maintenance once in a year for complete ICT infrastructure in off-peak hours, which will include the following:
   - Diagnostic tests to check all servers by running the console diagnostics tests to check hardware (CPU, Memory and I/O controllers).
   - Diagnostic tests to check SAN Storage status, like, Hard drive Status, Controller Status, Disk Enclosure Status, SAN Switch Status, loop Switch Status, Cache module and battery status, link Status between disk enclosure to array controller, fan Status, etc. The test should include environmental conditions like power supply, etc. and operational issues like space management.
   - Diagnostic tests to check and verify good health of all network and security equipment (CPU and/or other processors, RAM, Flash memory, NV RAM, network ports, various functional modules etc.)
   - Shall use diagnostic software or alternative facility/facilities to diagnose and analyze predictive failures in the disk drive of servers and storage.
   - Check and clean fan/blowers and power supplies for proper functioning
   - Perform physical inspection to see that all peripheral devices (e.g. DAT Drives etc.) are in no fault condition.
   - If any fault is detected during diagnostics then take necessary steps to rectify it and replace it, if required.
   - Analyze error log for errors reported since previous Preventive Maintenance activity.
   - If any errors are observed in error log, analyze them in detail and carry out necessary activities to eliminate them.
   - Collect data for all controllers and record in the site log
   - Preventive Maintenance (PM) report, which highlights the findings & follow-up actions, will be furnished to RailTel Customer within one week.

3) <u>Operating System Administration (Windows and Non-Windows)</u>

a) Installation, configuration, fine tuning, troubleshooting and maintenance Managing Windows and non-windows operating systems and Server Software

b) The Server software may include, but not limited to, web server, application server, E-mail servers, DNS servers, DHCP Server, Proxy servers, patch management server, anti-virus servers, FTP servers, LDAP/Active Directory servers etc.

c) Installation, configuration, fine tuning, troubleshooting and maintenance of Server Virtualization infrastructure

d) User management including user registration, user ID creation, maintaining user profiles, granting user access, authorization, user password support etc.

e) Writing Shell script for batch programming & system monitoring.

f) Ensure proper configuration of server parameters, operating systems administration and tuning as per defined guidelines.

g) OS migration to higher versions, whenever required.

h) Tracking, testing & installation of OS patches to ensure that the system is properly updated.

i) Implement and maintain Standard Operating Procedures based on the policies formulated in discussion with RailTel Customer and industry best practices / frameworks.

j) System Configuration Security hardening as per system hardening standard formulated in discussion with RailTel Customer in line with industry best practices / frameworks

k) Regularly monitor, maintain, analysis System logs of the performance monitoring of servers including but not limited to monitoring CPU, disk space, memory utilization, I/O utilization, etc. and produce adequate reports as defined and required by RailTel Customer.

l) Regularly monitor, maintain, analysis of Security logs of servers for security events and reporting of all security events to RailTel Customer

m) Take appropriate steps to comply with the audit observations made by various internal/ external auditors.

n) Ensure that the bottlenecks in the infrastructure are identified and fine-tuning is done for optimal performance.

o) Resolve any issues/incidents and carry out required changes, optimizations and modification.

p) Regular backup of servers (data and configuration) as per backup policies of the RailTel Customer using backup tools supplied by the bidder.

q) Regular analysis of events and logs and maintain the reports for future audit purposes.

r) Quarterly (or as required by RailTel Customer) review of domain level rights and privileges.

s) Maintaining/updating the documents on system configuration, process/procedures, user-manuals etc. related to the activities involved in.

t) Maintenance & Management of Hardware resources and coordinate with hardware vendors & troubleshoot any issue.

4) **<u>Application Server (Middleware) Maintenance</u>**

a) Installation of application server/middleware like WebLogic and OHS Server, or any other middleware as per RailTel Customer requirements

b) Configuration and management of managed server in WebLogic server.

c) Deployment of web application in Weblogic server.

d) Installation of tomcat and apache server.

e) Deployment of web application in tomcat server.

f) Installation of PHP and My SQL server.

g) SSL configuration on the websites.

h) Server health check-up

i) Monitoring of various websites.

j) Monitoring of bookings.

k) Resolving different server related issues

l) Resolving client issues.

m) Static website changes.

n) Providing application logs to the development teams.

o) Installation, configuration and management of SVN server.

p) To make daily reports of booking, PG success rate etc.

q) To upload images, mailers provided by portal team.

r) To provide data.

s) To provide different port access to all the related teams.

t) Monitoring of online users on Air website using google analytics.

u) Logs backup, application code backup.

5) **<u>Database Administration</u>**

a) Checking CPU Health, Space Monitoring, Server Accessibility
b) Checking alert log of all production database as well as staging database, Tablespace Monitoring, DB user expiration, Listener and connectivity
c) DB memory tuning like SGA, PGA, Managing server processes and sessions.
d) Create SQL query as per developer /operation team requirement, perform alter/update as per requirement.
e) Taking Backup on daily basis for all prod server as per RailTel Customer data backup policy.
f) Restore database/tables as per requirement.
g) Generate AWR/ADDM report and analyze the same to find root cause of issue.
h) As per requirement deploy new database server and configure the same for production.
i) Meeting/Discussion with Developer and as per requirement resolve developer query, Making Trigger/Procedure etc.
j) Time to time plan a host reboot activity to remove Zombie/slip process.
k) Checking Application concurrent number of process and session and if any process/session goes stuck or not responding, then kill the same process.
l) Password management as per RailTel Customer policy.
m) Make database cloning as per requirement.
n) Maintain a standby copy of all production servers for hardware failure or any outage regarding corruption.
o) Maintain and monitor Golden Gate configuration to continuous sync AIR/TOURISM profile data.
p) Making various type of shell scripting to execute a job in scheduled time and get appropriate data.
q) Regularly dump IPAY recon data into a table and maintain the same.
r) Maintain booking SMS data for nget,air,tourism,android etc.

6) **<u>Backup & Restoration Management</u>**

a) Maintenance of Backup server solution, Tape Library (TL) setup, Tape Library drives sharing, SAN client setup on Heterogeneous Operating Systems, Configuration of backup over LAN and SAN.
b) Regular backup and restoration of RailTel Customer data maintained in SAN storages/File Servers, and standalone servers in accordance with Data Backup policy of RailTel Customer including scheduled drill operations and on-demand operations.
c) Monitoring and enhancing the performance of scheduled backups, schedule regular testing of backups.
d) Maintaining index and logs as per retention policies.
e) Analysing the OS & Backup logs, alert logs, warning logs and other trace files and diagnosing problems.
f) Regular monitoring, log maintenance and reporting of backup status on a regular basis.
g) Periodic Restoration Testing of the Backup.
h) Report Generation and alerting on backup jobs.
i) Maintaining/updating the documents on backup configuration, procedures, user-manuals etc. related to backup & restoration activities.

7) **Backup Media Management**

a) Media Management with proper Retention period, including tagging, cross-referencing, storing, logging, testing, and vaulting of Tapes in safe cabinets (onsite and offsite). Safe cabinet shall be provided by RailTel Customer for this purpose

b) Maintaining inventory of on-site (IDC) and offsite (Internet Ticketing Center) tapes.

j) Tape/ LTO library management – loading and unloading tapes, etc.

k) Coordinating to retrieve off-site media in the event of any disaster recovery.

l) Forecasting and raising indent for tape requirements for backup.

8) **SAN Storage Maintenance**

a) Fault, availability, capacity and performance monitoring of SAN Storage Systems

b) Management of space, SAN/NAS volumes, RAID configuration, LUN, zone, security, business continuity volumes, performance etc.

c) Create/delete, enable/disable zones in the storage solution

d) Create/delete/modify storage volumes in the storage solution

e) Create/delete, enable/disable connectivity and access rights to storage volumes in the storage solution.

f) Fibre Channel (FC) switch configuration, firmware up-gradation, zoning and monitoring.

g) Troubleshooting & diagnosing issues related to Storage, backup and tape libraries.

9) **Network and IT Security Administration**

a) Installation, configuration, fine tuning, troubleshooting, integration and maintenance of entire Network & IT Security Infrastructure of RailTel Customer

b) Configuration, integration and management of Network Management System (NMS) ensuring proactive monitoring (fault, availability and performance) of entire ICT Infrastructure.

c) Configuration, integration and management of PIM solution supplied by the bidder, security policy management, fine-tuning and ensuring secure network access to RailTel Customer network.

d) Configuration and fine-tuning of routing protocols primarily BGP and OSPF etc., and high availability features like VRRP/HSRP, port aggregation etc.

e) Configuration of VLANs, NATing, NetFlow/ JFlow, IPsec VPN tunnel on network devices.

f) Coordination with third-party vendors like Telco, ISPs, etc. for installation, configuration, tuning, troubleshooting incidents and performance issues, and maintenance of network services like Internet Leased Lines, Point-to-point Leased Lines, MPLS, and DNS Services etc.

g) Coordination with third-party vendors like Managed Security Services Provider (MSSP) for SOC services, DDoS mitigation Services etc. as well as with Govt. agencies like CERT-In for security monitoring of RailTel Customer Infrastructure.

h) Management of users, processes, and system resources ·

i) OS migration to higher versions, whenever required.

j) Tracking, testing & installation of OS patches to ensure that the system is properly updated.

k) IP address management of entire ICT Infrastructure.

l) Physical labelling of each network equipment, ports and cables

m) Regular backup of OS and device configuration files.

n) Regularly monitor, maintain, analysis System logs of the performance monitoring of devices and servers including but not limited to monitoring CPU, disk space, memory utilization, I/O utilization, etc. and produce adequate reports as defined and required by RailTel Customer.

o) Regularly monitor, maintain, analysis of Security logs of devices and servers for security events and reporting of all security events to RailTel Customer

p) Monitoring and optimizing the LAN and WAN traffic

q) System Configuration Security hardening as per system hardening standard formulated in discussion with RailTel Customer in line with industry best practices / frameworks

r) Implement and maintain Standard Operating Procedures (Sops) based on the policies formulated in discussion with RailTel Customer and industry best practices / frameworks.

s) Quarterly review of devices configuration, network access permissions, ACLs, and firewall rule base etc.

t) Maintenance and regular update of documentation, reports and checklists related to Network architecture & diagrams, SoPs, Secure Configuration Hardening standard, Change control, Performance, availability and fault monitoring of ICT Infrastructure.

u) Take appropriate steps to comply with the audit observations made by various internal/ external auditors.

v) Identify bottlenecks in the infrastructure and perform fine-tuning for optimal performance.

w) Resolve any issues/incidents and carry out required changes, optimizations and modification.

10) <u>Host Security Management at Server Level</u>

a) Managing Host Security Software (Anti-virus + HIPS + Host firewall etc.) on Servers.

b) Virus detection, eradication, virus signature/definition synchronization across servers

c) Keep all the servers updated with the latest virus definition.

d) Problem analysis and its resolution related to Endpoint Security Software.

e) Periodic review and reporting of logs and corrective action.

f) Diagnose and rectify any virus/worm problems, which can be fixed by Endpoint Security Software.

g) Provide feedback to RailTel Customer on any new viruses detected or possible virus attack and take up promptly with OEM/ Support vendor for getting the appropriate patch and carry out the timely maintenance.

11) <u>Third-Party Vendor Management</u>

a) Coordination with all the third-party vendor/service providers of RailTel Customer for support services for maintenance of ICT infrastructure ensuring problems and issues are resolved in accordance with SLA of the vendor. These vendors may include, but not limited to, hardware vendors, Telco/ISPs, application management vendor, data centre service provider, software vendors etc.

b) Logging calls, co-ordination and follow-up with vendor. Escalation of calls to the higher level management on the vendor’s side, if need arises. Ensure that unresolved items are escalated in accordance with the escalation matrix shared by such vendors.

c) AMC/ Warranty/ Support Tracking

d) Tracking of assets sent for repair.

e) Maintain SLA and Escalation matrix for all these vendors with details like contact person, telephone nos., response time and resolution time commitments etc.

f) Tracking of SLA performance for all such vendors and submission a consolidated quarterly SLA performance report of these vendors for considerations of RailTel Customer.

12) Coordination for Third-Party Security Audits

a) RailTel Customer may conduct regular (half-yearly/annual) security audit of its ICT Infrastructure through third-party security auditor for vulnerability assessment & penetration testing of its web application and servers/devices, process audit for the security practices, implementation of security policy & procedures. The bidder shall provide necessary support and co-operation for these audits, and implement all the audit recommendations in time as agreed upon with RailTel Customer.

13) Remote Hands Support at RailTel IDC

a) Reboot of a ICT equipments including servers

b) Providing system console access of the ICT equipments.

c) Powering on/off the ICT equipments.

d) Inserting and removing media, Tapes (CDs etc.) for installation of software/OS.

e) Maintaining physical connections of the cables (data & network)

f) Provide secure access i.e. escorted entry to ICT equipments for RailTel Customer's employees and / or RailTel Customer’s vendor for maintenance purpose, after approval of RailTel Customer.

g) Keep track of the ICT assets colocated in the Data Center.

h) Facilitate entry and exit of ICT equipment/parts and maintain in / out logs for equipment.

i) Handling and vaulting of backup media for IRCT data.

j) Monitoring of third-part vendors working in the server room on RailTel Customer ICT equipments.

k) Monitoring and Reporting the status of the equipment.

14) Asset Management

a) Regularly maintain the component-level inventory of the entire hardware and software in the ICT infrastructure at IDC facility.

b) Any discrepancy in software licenses available and actually used should be reported to avoid any software piracy.

c) Maintaining all documentation related to material movement such as new hardware, spare parts or equipment going out of premises for repairing or replacement etc.

15) Management Information System (MIS) Reporting and Documentation

a) Preparation, maintenance and submission of various MIS reports as per requirements of RailTel Customer on regular basis RailTel Customer in mutually decided format. The following is only an indicative list of MIS reports.

- Daily reports
  - Summary of issues/complaints logged at the Help Desk
  - Summary of resolved, unresolved and escalated issues/complaints
  - Summary of resolved, unresolved and escalated issues/complaints to OEMs/third-party vendors.
  - Log of data and configuration backup and restoration undertaken.
  - Log of Incidents - Operational and Security Incidents reports

- Weekly Reports
  - Issues /Complaints Analysis report from Help Desk.
  - Summary of issues / complaints logged with the OEMs/third-party vendors.
  - Summary of changes undertaken in the ICT Infrastructure including major changes like configuration changes, patch upgrades, database reorganization, storage reorganization, etc. and minor changes like log truncation, volume expansion, user creation, email ID creation, user password reset, etc.
  - Summary of Incident report along with RCA, plan of avoidance, reporting for repetition of similar incident
- Monthly reports
  - Component wise ICT infrastructure availability, performance and capacity utilization.
  - SLA / non-conformance report – Bidder Agency.
  - SLA / non-conformance report – Third-party vendors/service providers
  - Summary of On-line Services uptime (like Air Booking, Tourism Services etc.).
  - Summary of component wise ICT infrastructure uptime.
  - Change Management report
  - Access management report
  - Consolidated Summary of Incident report along with RCA, plan of avoidance, reporting for repetition of similar incident
  - Log of preventive /scheduled maintenance undertaken
  - Log of break-fix maintenance undertaken
  - Attendance record and time sheet of bidder's staff deputed at RailTel Customer.
  - Consolidated backup and restoration undertaken.
- Quarterly Reports
  - Consolidated component-wise ICT Infrastructure availability, performance and capacity utilization.
  - Consolidated On-line Services uptime (like Air Booking, Tourism Services etc).
  - SLA / non-conformance report – Bidder Agency.
  - SLA / non-conformance report – Third-party vendors/service providers
  - Firewall Rule-base Review report
  - Configuration Hardening Compliance
  - Warranty/AMC/Subscription Support Status
  - Asset management report
  - Consolidated Access management report
  - Consolidated preventive/scheduled and break-fix maintenance undertaken
  - Software license compliance reports
- Half-yearly Reports
  - ICT infrastructure Upgrade / Obsolescence Report
  - Asset management report
- Incident Report
  - Operational Incident reports
  - Security Incidents reports
  - Software license violations reports
  - Miscellaneous incident reports

Annexure-6: Service Levels & Penalties

SERVICE LEVELS AND PENALTIES

This section clearly defines the levels of service which shall be provided by Bidder to RailTel Customer for the duration of contract.

1. OBJECTIVE:

The objectives of this Service Level Agreement are to:

a) Trigger a process that applies RailTel and Bidder management attention to some aspect of performance when that aspect drops below an agreed upon threshold, or target.

b) Makes explicit the expectations that RailTel Customer has for performance.

c) Helps RailTel Customer control the levels and performance of RailTel services.

2. DEFINITIONS

For purposes of this Service Level Agreement, the definitions and terms as specified in the contract along with the following terms shall have the meanings set forth below:

- ***"Availability/Uptime"*** shall mean the time for which the Services/Systems maintained by Bidder are available for conducting intended operations. Uptime/Availability of Services/equipment shall be calculated as:

  Availability = {(Total Availability Time – Downtime) / Total Availability Time)}*100

- ***"Incident"*** refers to any event / abnormalities in the functioning of the ICT Infrastructure and services that may lead to disruption to normal operations of RailTel Customer business and infrastructure services and IT Operations.
- "**Downtime"** shall be the time from the point the respective service/equipment becomes unavailable to the intended user(s) till the time the same becomes fully available.
- ***"Resolution Time***" means time taken by the RailTel to detect the incident till the time the problem has been fixed.

3. DESCRIPTION OF SERVICES PROVIDED

The exact scope and boundaries of services provided as part of this agreement are detailed in **Section 2: Scope of Work** and Annexures therein of this tender.

4. MEASUREMENTS & TARGETS:

This SLA document provides for minimum level of services required as per contractual obligations based on performance indicators and measurements thereof. RailTel shall ensure provisioning of all required services while monitoring the performance of the same to effectively comply with the performance levels.

The SLA has been categorized into following categories:

A. Data Center Colocation Services Related Service Levels

B. Equipment Availability/Uptime and Performance Related Service Levels for ICT Items supplied by Bidder

C. Connectivity Related Service Level

D. O&M Related Service Levels

The following measurements and targets shall be used to track and report performance on a regular basis. The targets shown in the following table are applicable for the duration of the contract. However, these SLAs are subject to revision or rectification with mutual agreement between RailTel Customer and RailTel.

A. Data Center Colocation Services – Service Level and Penalties

Data Center Colocation Services will be measured on the basis of the following SLA Objectives: Power Availability, Environmental Control, and Physical Security. These SLA Objectives are applicable on a 24 hour a day, 7 days per week basis.

A.1 Power Availability:

Uptime (%) per Month	Penalty as % of MRC DC Colocation Services for each affected rack
>= 99.982	Nil
>= 99.90 and < 99.982	5%
>= 99.80 and < 99.90	10%
>= 99.70 and < 99.80	15%
>= 99.50 and < 99.70	30%
Below 99.50%	50%

**** MRC: Monthly Recurring Charges***

A.2 Environmental Control Availability:

Control	Monthly SLA Target	SLA Breach	Penalty as % of MRC DC Colocation Services
Temperature	Up to 24 (+/- 2) Degree Celsius	Not within specified limit continuously for 30 minutes	5% for each 60 minute increment of aggregate breach up to a maximum of 50% per month
		More than 4 breaches in a month	50%
Humidity	50 (+/- 10)	Not within specified limit continuously for 30 minutes	5% for each 60 minute increment of aggregate breach up to a maximum of 50% per month
		More than 4 breaches in a month	50%

A.3 Physical Security

SLA Objective	SLA Target	Penalty
Physical Security	No Unauthorized Access	50% of MRC for total DC Colocation Services for a month in which any unauthorized access occurred.

B. ICT Infrastructure Uptime – Service Level and Penalties

i. **Total Service Failure:** Bidder shall provide system uptime guarantee of **99.6%** on monthly basis. The system will be treated as 'down' (termed as 'Total Service Failure') in case of failure of one or multiple services of RailTel Customer, hosted in the RailTel IDC, due to failure / misbehaviour of any of the equipment/s including Firewalls, ADC, Core Switches, and Internet Gateway Routers, maintained in High-availability/Custer mode as well as Server virtualization infrastructure, supplied and maintained by RailTel.

Non-availability/failure of complete cluster of these equipment/s (in HA) due to power/cooling failure shall also be treated as ‘Total Service Failure’.

Also, in case of failures exceeding the defined uptime for the month, it shall attract penalties as defined in the table given below. Irrespective of the duration of failures, if there are more than 02 failures in a month, this too shall be treated as *Total Service Failure* and

Any incident of ‘Total Service Failure’ shall attract penalties as defined in the table given below.

ii. **Equipment failure**: In addition to the above, in case of failure of any equipment (Routers, Switches, ADC, Next Generation Firewall etc.), supplied by Bidder, the equipment shall be replaced by Bidder by the end of Next Business Day (NBD).

If the number of failures of any equipment exceeds 02 in a month or the duration of failure exceeds the NBD window, it shall attract penalties as defined in ‘Equipment failure’ in the table given below. For the purpose of calculating the penalty, the excess failure time shall be counted but in case number of failures exceed more than the permissible limit, complete failure period shall be counted for calculation of penalty.

Any incident of ‘Equipment Failure’ shall attract penalties as defined in the table given below.

iii. The planned downtime or downtime on account of failure of equipment/software not supplied by the Bidder (excluding OS Licenses) will not be considered for calculating uptime, but in case of planned downtime exceeding the allotted downtime or the activity resulting in some system failure /equipment failure then the system shall be treated as down and it shall attract penalties given in the “Total Service failure” item or the item “Equipment failure” of the table given, as applicable.

iv. Penalties shall be calculated on the basis of ‘Total Service Failure’ as well as individual ‘Equipment Failure’. In case both are applicable for same duration, the higher one shall be charged.

v. Root Cause Analysis of all failures – a preliminary report shall be submitted by RailTel within 24 hours of the failure and a detailed technical analysis report on the root cause from OEM shall be submitted within one week from the date of failure.

Uptime SLA Failure	**Penalty**
Total Service failure	Rs. 01 Lakh per hour of downtime, exceeding the defined SLA (on pro rata

	basis).
Equipment failure – Critical (Firewall, ADC, Core L3 Switches, Router (Internet) and PIM)	Rs. 30,000 /- per day of downtime, exceeding the defined SLA (on pro rata basis).
Equipment failure (Others)	Rs. 15,000 /- per day of downtime, exceeding the defined SLA (on pro rata basis).

C. O&M Services – Service Level and Penalties

S. No.	Measurement	Definition	Measurement Interval	Target SLA	Penalty (as % of Quarterly O&M Services Charges) for every non-compliance
1.	Change Management	Measurement of quality and timeliness of changes to the ICT Infrastructure at IDC and ITC facilities	Quarterly	100% of changes should follow formal change control procedures. All changes need to be approved by RailTel Customer.	**0.2%**
2.	Scheduled Maintenance	Measures timely maintenance of the ICT Infrastructure equipment. RailTel shall provide a detailed Maintenance plan for each maintenance activity.	Quarterly	90% of scheduled Maintenance should be carried out as per Maintenance plan submitted by Bidder.	**0.5%**
3.	Implementation of Security Audit Recommendations	Implementation of Audit recommendations for remediation of audit gaps made by auditors, as per agreed timelines	Quarterly	To be Implemented as per timelines agreed upon with RailTel Customer.	**2%**
4.	Preventive Maintenance (PM)	Preventive Maintenance of Systems supplied & maintained by the Bidder, as per agreed timelines	Bi-Annual	After every six months	**5%**
5.	Incident Reporting	Reporting of Availability/ Fault related incidents to RailTel Customer	Quarterly	90% of the incidents to be reported with-in 30 minutes of	**0.2%**

S. No.	Measurement	Definition	Measurement Interval	Target SLA	Penalty (as % of Quarterly O&M Services Charges) for every non-compliance
				failure.	
6.	Logging Incident/Fault Cases	Logging of Incident/Fault case, after preliminary examination, to OEM/Service Providers by Bidder Help Desk for troubleshooting and resolution for complete ICT infrastructure (including ICT infrastructure not supplied but monitored by RailTel) of RailTel Customer hosted at IDC.	Quarterly	90% of the faults to be logged with OEM/ Service Providers with-in one hour of failure.	**0.2%**
7.	Manpower availability	Required number of shift should be manned with minimum nos. of qualified engineers	Quarterly	100% availability on shift basis	Deduction of cost of manpower on pro-rate basis.

5. <u>SLA PENALTIES</u>

a) Total penalty in a quarter for failure to maintain the promised Service levels shall be subject to a maximum of **10%** of the total quarterly recurring cost payable to Bidder.

b) In case of two consecutive quarterly deductions of **10%** of the total quarterly recurring cost, RailTel reserves the right to cancel the contract in whole or in part thereof and/or confiscate the Security Deposit and/or PBG Bond.

c) Following shall be excluded from the downtime –

- Scheduled or Emergency Downtime
- Downtime on account of failure of ICT components not supplied by the Bidder or not under AMC support of the Bidder, subject to timely incident reporting and call logging by RailTel
- Force Majeure or any Governmental or court order

However, in case of Scheduled downtime exceeding the allotted downtime window or the activity resulting in some system or service failure /equipment failure, then the services/system shall be treated as down and it shall attract penalty as applicable.

d) Penalties shall be cumulative i.e., penalties on account of different failures shall be deducted in total. However, in case of single failure resulting from multiple incidents, higher of the penalties shall be deducted.

e) SLA Penalties shall be deducted from Invoices/bills to be raised by the Bidder on quarterly basis. RailTel Customer also reserve the right to deduct the penalties from Security Deposit and/or PBG submitted by Bidder.

Annexure-7: Existing ICT Infrastructure

Existing Hardware items at ITC that are to be migrated to RailTel IDC

S. No.	Item Description*	Make & Model	Qty
1.	SAN Storage Mgmt. Server	HP 3PAR Store Server	1
2.	SAN Switch	HP SN3000B 24/24 FC Switch	2
3.	Tape Library	HP MSL 2024 0-Drive	1
4.	Data Protector Server	HP Data Protector for Tape Backup	1
5.	Blade Servers	HP ProLiant BL 460c Gen 8	43
6.	Blade Chassis Enclosure	c7000	4

*RailTel shall collect component level inventory details from RailTel Customer.

Service Levels and Penalties

Refer Annexure-6: Service Levels and Penalties for details.

Annexure-8: Existing ICT Infrastructure

Bidder shall commission the supplied products in a period of **18 weeks** from the date of award of Purchase Order. Implementation process and Project schedule shall be executed in two phases:

- Phase-I: Supply an implementation of basic ICT infrastructure and migration activities for migration of all critical ICT infrastructure and application from Internet Ticketing Center.
- Phase-II: Implementation of ICT items that are presently not running at ITC DC facility and are procured under this tender separately.

Important milestones are given as below:

S. No.	Milestone	Weeks from date of award of Purchase Order to RailTel
1.	System Study and finalization of Systems Deployment Architecture	2
2.	• Submission of detailed Project Plan, including migration plan, detailing each task with target date and assigned resource persons including the plan for installation of all supplied items and integration with existing infrastructure. • Submission of HP Hardware migration plan • Submission of Email Servers migration plan	3
3.	Supply of all ICT Items as specified in Table-A of Schedule of Rates	8
4.	Migration and installation of existing SAN Storage System to IDC	8 (In parallel)
5.	Provisioning of Internet Bandwidth Services with DDoS Protection	8 (In parallel)
6.	Provisioning of Point-Point Leased Services	8 (In parallel)
7.	Phase-I a) Installation and configuration of all supplied ICT Items, except the following items, and submission of installation report. i. Anti-APT ii. PIM iii. 2FA iv. Help Desk & NMS b) Installation and integration of new server hardware, including Blade Chassis, Blade Servers and Rack Servers to be procured by RailTel Customer directly through separate sourcing process, with new supplied ICT items and SAN Storage, and ensuring the readiness of ICT Infrastructure (network & security, server and storage system) ready for migration of RailTel Customer application to IDC facility. c) Acceptance on Installation and Integration by RailTel Customer	10
8.	Migration of all business applications and database of RailTel Customer being managed by RailTel from ITC to IDC.	12
9.	Migration of existing servers at ITC to IDC	14
10.	Migration of remaining services – Portal, ERP, Email, SMS etc..	(In parallel)

11.	Phase-II a) Installation, configuration and integration of the following items, and submission of installation report. i. Anti-APT Solution ii. PIM iii. 2FA iv. LDAP/IDM v. Help Desk & NMS b) Execution of Acceptance Test Procedure (ATP).	18
12.	**Commissioning of System and O&M Services**	18

Penalty on delay in System Commissioning:

a) In the event of Bidder’s failure to successfully commission the systems and O&M Services within agreed schedule as detailed above, penalty shall be levied on Bidder @ 0.5% of the “Sum of Total Value of Table-A, B and C) of Annexure-3” for delay in system commissioning.

b) Delay on part of RailTel shall not be accounted on Bidder’s part.

Annexure-9: Non-Disclosure Agreement

(This NDA shall be executed on Non-Judicial Stamp Paper of Rs. 100 value)

CONFIDENTIALITY - CUM - NON-DISCLOSURE AGREEMENT (NDA)

THIS NON-DISCLOSURE AGREEMENT is made on this …..…….. day (date) of ……….. (Year)

By and between

'RailTel Corporation of India Limited', a Public Sector Undertaking (PSU) under Ministry of Railways, having its Corporate Office at Plot No.-143, Sector44, Institutional Area, Opposite Gold Souk Mall, Gurgaon, Haryana-122003 (hereinafter referred to as "**RailTel**" which expression shall unless repugnant to the context or meaning thereof, includes its successors, administrators and permitted assigns) of the FIRST PART.

And

………………………………*<Name incorporated/registered>* under the………..…...*<Name of the Act>* having its registered/corporate office at ……...……………… (herein referred to as "**Recipient**" which expression shall unless repugnant to the context or meaning thereof, includes its successors, assigns, administrators, liquidators and receivers) of the SECOND PART.

WHEREAS

A. Recipient's services have been hired by RailTel for "………………..." (Authorized purpose) vide Agreement/Purchase/Work Order No……. dated………….

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

1. **Definitions:**
   a) The term "Confidential Information" shall include, without limitation, all technical and non-technical information and materials, furnished by RailTel or any of its associated partners on behalf of RailTel to the Recipient in connection with RailTel products and services including information transmitted in writing, orally, visually, (e.g. video terminal display) or on magnetic media, and including all information marked as 'Confidential' or 'Sensitive' or 'Proprietary', customer & prospect lists, personal data of RailTel employees and its customers, trade secrets, trade names or proposed trade names, methods and procedures of operation, business or marketing plans, licensed document know-how, ideas, concepts, designs, drawings, flow charts, diagrams, quality manuals, checklists, guidelines, processes, formulae, source code materials, specifications, programs, software packages, codes and other intellectual property relating to RailTel products and services. Results of any information security audits, tests, analysis, extracts or usages carried out by the Recipient in connection with the RailTel's products and/or services, IT infrastructure, etc. shall also be considered Confidential Information.
   b) The term "RailTel products" shall include all such products, goods, services, deliverables, which are subject to deliver, install and/or be maintained by the Recipient under the Agreement.

2. **Protection of Confidential Information.** Recipient affirms that it shall:

a) Use the Confidential Information only to the extent necessary to accomplish '*Authorized purpose*' and in accordance with the terms and conditions contained herein;

b) Maintain the Confidential Information in strict confidence and take all reasonable steps to enforce the confidentiality obligations imposed hereunder, but in no event take less care with the Confidential Information that the recipient takes to protect the confidentiality of its own proprietary and confidential information and that of its other clients;

c) Not make or retain copy of any details of products and/or services, prototypes, business or marketing plans, Client lists, Proposals developed by or originating from RailTel or any of the prospective clients/partners of RailTel.

d) Not make or retain copy of any details of results of any information security audits, tests, analysis, extracts or usages carried out by the Recipient in connection with the RailTel's products and/or services, IT infrastructure, etc. without the express written consent of RailTel.

e) Not disclose or in any way assist or permit the disclosure of any Confidential Information to any other person or entity without the express written consent of the RailTel;

f) Immediately notify RailTel in writing upon the discovery of any loss or unauthorized disclosure of any confidential information.

g) Return to the RailTel, or destroy, at RailTel's discretion, any and all Confidential Information disclosed in a printed or electronic form or other permanent record, or in any other tangible form (including without limitation, all copies, notes, extracts, analyses, studies, summaries, records and reproductions thereof) immediately on (i) expiration or termination of this agreement, or (ii) the request of RailTeltherefor.

h) Not send RailTel's information or data and/or any such Confidential Information at any time outside India for the purpose of storage, processing, analysis or handling without the express written consent of the RailTel.

i) Use only the best possible secure methodology to avoid confidentiality breach, while handling confidential data of RailTel for the purpose of storage, processing, transit or analysis including sharing of information with RailTel.

j) Not to engage or appoint any non-resident/foreigner to undertake any activity related to Information Security Audit in respect of RailTel/ Government/ critical sector organization. Only the man power declared to CERT-In shall be deployed to carry out such audit related activities.

k) Not discuss with any member of public, media, press, any or any other person about the nature of arrangement entered between the Recipient and RailTel or the nature of services to be provided by Recipient to RailTel.

l) Make sure that all the employees and/or consultants engaged by Recipient to undertake any audit or services as part of '*Authorized purpose*' as specified above on its behalf have signed the mandatory non-disclosure agreement.

3. **Permitted disclosure of Confidential information:** If the recipient is requested/required to disclose confidential information by law enforcement or similar Government agencies mandated under the law, it is agreed that the receiving party shall provide RailTel with prompt notice of any such request or obligation so that RailTel may seek an appropriate protective order and or wave the recipient compliance with the provision of this agreement.

4. **Title and Proprietary Rights:** Notwithstanding the disclosure of any confidential information by RailTel to the recipient, the title and all intellectual property and proprietary rights in the confidential information shall remain with RailTel. The provisions of this agreement are necessary for the

protection of the business goodwill of RailTel and are considered by RailTel to be reasonable for such purposes. Recipient agree that any breach of this agreement will cause substantial and irreparable damages to RailTel.

5. **Exceptions.** The Confidentiality obligations as enumerated in Article 2of this Agreement shall not apply in following cases:
   a) Which is independently developed by Recipient or lawfully received from another source free of restriction and without breach of this Agreement; or
   b) After it has become generally available to the public without breach of this Agreement by Recipient; or
   c) Which at the time of disclosure to Recipient was known to such party free of restriction and evidenced by documents in the possession of such party; or
   d) Which RailTel agrees in writing is free of such restrictions.
   e) Which is received from a third party not subject to the obligation of confidentiality with respect to such Information;

6. **Onus.** Recipient shall have the burden of proving that any disclosure or use inconsistent with the terms and conditions hereof falls within any of the foregoing exceptions.

7. **Remedies.** Recipient acknowledges that any actual or threatened disclosure or use of the Confidential Information by Recipient would be a breach of this agreement and may cause immediate and irreparable harm to RailTel or to its clients/partners; Recipient affirms that damages from such disclosure or use by it may be impossible to measure accurately; and injury sustained by RailTel/ its clients/partners may be impossible to calculate and compensate fully. Therefore, Recipient acknowledges that in the event of such a breach, RailTel shall be entitled to specific performance by Recipient of its obligations contained in this Agreement. In addition, Recipient shall compensate the RailTel for the loss or damages caused to the RailTel actual and liquidated damages which may be demanded by RailTel. Liquidated damages not to exceed the Contract value. Moreover, RailTel shall be entitled to recover all costs of litigation including reasonable attorneys' fees which it or they may incur in connection with defending its interests and enforcement of contractual rights arising due to a breach of this agreement by Recipient. All rights and remedies hereunder are cumulative and in addition to any other rights or remedies under any applicable law, at equity, or under this Agreement, subject only to any limitations stated herein.

8. **Need to Know.** Recipient shall restrict disclosure of such Confidential Information to its employees and/or consultants with a need to know (and advise such employees and/or consultants of the obligations assumed herein), shall use the Confidential Information only for the purposes set forth in the Agreement, and shall not disclose such Confidential Information to any affiliates, subsidiaries, associates and/or third party without prior written approval of the RailTel. No information relating to RailTel shall be hosted or taken outside the country in any circumstances.

9. **Intellectual Property Rights Protection.** No license to a party, under any trademark, patent, copyright, design right, mask work protection right, or any other intellectual property right is either granted or implied by the conveying of Confidential Information to such party.

10. **Ownership:** the confidential information is the property of RailTel or its associates or advisors. Nothing in this agreement shall be construed as granting any property rights, by license or otherwise, to any confidential information disclosed pursuant to this agreement or to any invention or any patent, copyright, trademark, or other intellectual property right that has issued or that may issue, based on such confidential information. The recipient shall not make, have made, use or sell for any purpose any product or other item using, incorporating or derived from any confidential information. It is understood and agreed that neither party solicits any change in the organization, business practice, service or products of the other party, and that the disclosure of confidential information shall not be construed as evidencing any intent by a party to purchase any products or services of the other party nor as an encouragement to expend funds in development or research efforts. The confidential information may pertain to prospective or unannounced products. The recipient agrees not to use any confidential information as a basis upon which to develop or have a third party develop a competing or similar product.

11. **No Conflict.** The parties represent and warrant that the performance of its obligations hereunder do not and shall not conflict with any other agreement or obligation of the respective parties to which they are a party or by which the respective parties are bound.

12. **Authority.** The parties represent and warrant that they have all necessary authority and power to enter into this Agreement and perform their obligations hereunder.

13. **Publicity**: the recipient must not make any press or other public statements (which includes announcements and releases) relating to this agreement, the confidential information and the authorized purpose.

14. **Forum**: the recipient shall submit to the exclusive jurisdiction of the courts in Delhi, India to adjudicate any dispute arising out of this agreement.

15. **Communications**: Written communications requesting or transferring proprietary information under this agreement shall be addressed only to the respective designees as follows (or to such designees as the parties hereto may from time to time designate in writing)

    (Recipient)
    (Recipient's Address)

16. **Notices**: any notice required by this agreement or given in connection with it, shall be in writing and shall be given to the appropriate party by personal delivery or by certified mail, postage prepaid, or recognized overnight delivery services.

    If to RailTel:
    Dy General Manager/IT
    Plot No.-143, Sector44, Institutional Area, Opposite
    Gold Souk Mall, Gurgaon, Haryana-122003
    IF to Recipient:
    (Recipient)
    (Recipient's Address)

17. **Headings**: Headings used in this agreement are provided for convenience only and shall not be used to construe meaning or intent

18. **Governing Law.** This Agreement shall be interpreted in accordance with and governed by the substantive and procedural laws of India and the parties hereby consent to the jurisdiction of Courts and/or Forums situated at New Delhi

19. **Entire Agreement.** This Agreement constitutes the entire understanding and agreement between the parties on this subject, and supersedes all previous communications, both oral and written, representations and under standings among the parties with respect to the subject matter hereof.

20. **Amendments.** No amendment, modification and/or discharge of this Agreement shall be valid or binding on the parties unless made in writing and signed on behalf of each of the parties by their respective duly authorized officers or representatives.

21. **Binding Agreement.** This Agreement shall be binding upon and inure to the benefit of the parties hereto and their respective successors and permitted assigns.

22. **Severability.** It is the intent of the parties that in case any one or more of the provisions contained in this Agreement shall be held to be invalid or unenforceable in any respect, such provision shall be modified to the extent necessary to render it, as modified, valid and enforceable under applicable laws, and such invalidity or unenforceability shall not affect the other provisions of this Agreement.

23. **Waiver.** Waiver by either party of a breach of any provision of this Agreement, shall not be deemed to be waiver of any preceding or succeeding breach of the same or any other provision hereof.

24. **Survival.** Both parties agree that all of their obligations undertaken herein with respect to Confidential Information received pursuant to this Agreement shall survive till perpetuity even after expiration or termination of this Agreement.

25. **Non-solicitation.** During the term of this Agreement and thereafter for a further period of two (2) years, Recipient shall not solicit or attempt to solicit RailTel’s employees and/or consultants, for the purpose of hiring/contract or to proceed to conduct business similar to RailTel with any employee and/or consultant of the RailTel who has knowledge of the Confidential Information, without the prior written consent of RailTel.

26. This Agreement is governed by and shall be construed in accordance with the laws of India.

27. **Term.** This Agreement shall come into force on the date of its signing by both the parties and shall be valid up to **Five years**.

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

For and on behalf of RailTel	**For and on behalf of RECIPIENT**
Name of the Organization: RailTel Corporation of India Limited (RailTel)	Name of the Organization:
Sign:	Sign:
Name:	Name:
Designation:	Designation:
Witnessed by:	**Witnessed by:**
Sign:	Sign:
Name:	Name:
Designation:	Designation:

****** End of document ******