West Bengal State Electricity Distribution Company Limited
(A Government of West Bengal Enterprise)
(IT Cell)
Vidyut Bhavan,3rd Floor, C&D Block, Bidhan Nagar, Block-DJ, Sec-II, Kolkata-700091
Phone No.033-23197445,
Website: www.wbsedcl.in, e-mail: network.itcell@wbsedcl.in
CIN: U40109WB2007SGC113473

WBSEDCL

Notice Inviting e-Tender

Implementation of SD-WAN, Managed Switch and Network Upgradation under WBSEDCL.

Estimated Tender Price: Rs 22,50,00,000/- (Rs Twenty-Two Crore Fifty Lakh only)

Tender Notice No: WBSEDCL/IT&C/6.10/2357 Dated: 12.02.2026

12/02/26

Chief Engineer,
IT Cell
WBSEDCL

DISCLAIMER

This Tender Document (also referred as "Request for Proposal" or "RFP") is not an agreement and is not an offer or invitation by WBSEDCL to any Bidder other than one that qualifies based on evaluation of submitted BIDs. The purpose of this tender document is to provide information to the potential Bidders to assist them in responding to this Tender Document. Though this Tender Document is prepared with sufficient care to provide all required information to the potential Bidders, they may need more information than that has been provided. In such cases, the potential Bidders are solely responsible to seek the information required from WBSEDCL, at their own price. WBSEDCL reserves the right to provide such additional information at its sole discretion. In order to respond to the Tender Document, if required, and with the prior permission of WBSEDCL, the potential Bidder may conduct his own study and analysis, as may be necessary.

WBSEDCL makes no representation or warranty and shall incur no liability under any law, statute, rules or regulations on any claim the potential Bidder may make in case of failure to understand the requirement and respond to the Tender Document. WBSEDCL may, in its absolute discretion, but without being under any obligation to do so, update, amend or supplement the information the information in this Tender Document.

CONTENTS

GENERAL INFORMATION

1. **About WBSEDCL** -West Bengal State Electricity Distribution Company Limited (WBSEDCL), a Government of West Bengal owned utility established through the unbundling of the erstwhile WBSEB, is responsible for distribution and hydro generation of electricity across the State and serves as the nodal agency for implementing rural electrification initiatives. The Company is committed to ensuring reliable, efficient, and consumer-centric power supply while continually strengthening its operational, administrative, and service delivery capabilities, including robust IT and network security controls. In pursuit of these objectives, WBSEDCL is undertaking large-scale digital transformation initiatives focused on process standardization, system automation, enhanced visibility, data-driven decision-making, and improved customer experience.

2. **Present Network overview**- WBSEDCL operates a state-of-the-art on-premises Data Centre (DC) along with a Disaster Recovery Centre (DRC). WBSEDCL currently operates a wide-area network comprising multiple MPLS connectivity links, Point to Point links and internet links from different service providers across its Data Centre (DC), Disaster Recovery (DR), and field/site offices spread throughout West Bengal.

   Several mission-critical and enterprise applications are hosted centrally at the Data Centre (DC) and Disaster Recovery Centre (DR) and are accessed by approximately 700 WBSEDCL locations interconnected mainly through the existing MPLS network. In addition to the on-premises infrastructure, applications and services are integrated with cloud platforms for purposes such as hosting, disaster recovery, analytics, and application-specific requirements. Connectivity to these cloud resources is established through secure internet-based or leased connectivity, with appropriate security controls and government guidelines, and is expected to scale in line with WBSEDCL's needs.

3. **Objective of the NIT** - WBSEDCL intends to modernize its network environment to deliver enhanced security controls, high availability, improved performance, unified administration, and greater operational visibility by deploying SD-WAN, managed switching infrastructure, enterprise wireless solutions, NAC-AAA, centralized logging, reporting & analytics platforms, thereby supporting reliable internal operations and an improved experience for consumer-facing services.

   The objective is to establish secure and seamless connectivity among the Data Centre (DC), Disaster Recovery Centre (DRC), Headquarters (HQ), field offices, and integrated cloud-based applications/services, as per WBSEDCL's requirement.

   The functional and technical requirements/specifications for this project have been prepared based on

   - WBSEDCL's functional and security requirements, optimal utilization of resource,
   - Ensuring alignment with ISO 27001:2022,
   - CERT-In, NCIIPC, and other relevant Government of India security agency guidelines, as well as established industry best practices.

   These specifications are intended to ensure that the proposed network upgradation–related devices under this project meet the highest standards of performance, security, compliance, and operational efficiency.

SECTION: I
INSTRUCTION TO BIDDER (IB)

IB.1. West Bengal State Electricity Distribution Company Limited hereinafter referred to as WBSEDCL, a Govt. of West Bengal Enterprise is responsible to distribute uninterrupted and quality Power within the State of West Bengal, invites e-tender for "Implementation of SD-WAN, Managed Switch and Network Up-gradation under WBSEDCL", as per detailed "Scope of Work" and other terms and conditions furnished in the different clauses of the Bid Document.

IB.2. **Eligibility of Bidders:**

Following are the credentials for eligibility of Bidders:

IB.2.1. The bidder should be registered in India with the Registrar of Companies/Firms and possess a valid Corporate Identification Number (CIN).

IB.2.2. The bidder must possess a valid ISO 27001:2022 or latest certification throughout the project period.

IB.2.3. **SD-WAN Experience**:

i. The bidder must have successfully implemented and/or managed a minimum of 750 SD-WAN devices of same OEM, in the last seven (7) years from date of publishing of tender in one or maximum of two LOA's.

ii. For OEM – successful installation and operation of a minimum of **1500** SD-WAN endpoints (hardware/software) in the last seven (7) years from the date of publishing of the tender, executed under one (1) or a maximum of two (2) Letters of Award (LOA).

In addition, the OEM must have live and operational SD-WAN deployments as on the date of publishing of this tender, providing active support for a minimum of 500 SD-WAN boxes, over and above the above-mentioned deployments, executed under one (1) or maximum of two (2) Letters of Award (LOA).

IB.2.4. **Managed Switch Experience**:

i. The bidder must have successfully implemented and/or managed a minimum of 800 managed switches in the last seven (7) years from date of publishing of tender in one or maximum of two LOA's.

ii. For OEM -minimum 1500 managed switches in the last seven (7) years from date of publishing of tender in one or maximum of two LOA's.

In addition, the OEM must have live and operational Managed switch deployments as on the date of publishing of this tender, providing active support for a minimum of 500 managed switches, over and above the above-mentioned deployments, executed under one (1) or maximum of two (2) Letters of Award (LOA).

IB.2.5. **Agent-Based Deployments Experience**:

i. For bidder minimum 1000 client endpoints installation and management experience for NAC/AAA/EDR/any agent-based application etc in the

last seven (7) years from date of publishing of tender in one or maximum of two LOA's.

ii. For OEM minimum 15,000 NAC/AAA agents, in the last seven (7) years from date of publishing of tender in one or maximum of two LOA's.

In addition, the OEM must have live and operational NAC-AAA deployments as on the date of publishing of this tender, providing active support for a minimum of 1000 devices/users, over and above the above-mentioned deployments, executed under one (1) or maximum of two (2) Letters of Award (LOA).

IB.2.6. The bidder should have a minimum annual turnover of INR 100 crore (Rupees One Hundred Crore only) in each of the last three financial years ending on 31.03.2025 (i.e., FY 2022–23, 2023–24, and 2024–25).

IB.2.7. The bidder should have a positive net worth in each of the last three financial years, i.e., FY 2022–23, 2023–24, and 2024–25. Net worth certificate from any Chattered Firm to be submitted.

IB.2.8. The bidder should not have been blacklisted by any Government organization across India during the last three (3) calendar years. An undertaking to this effect shall be submitted by the authorized signatory of the bidder. If, at any time during the contract period, the submitted undertaking is found to be false, the purchase order/work order issued to the bidder shall be terminated, and the Bank Guarantee (BG) shall be forfeited.

IB.2.9. The bidder must have a valid agreement/partnership with the proposed SD-WAN OEM, network switch (Manager Switch) OEM, NAC-AAA OEM, Log server OEM and other relevant network equipment OEMs whose platforms are being offered for providing services to WBSEDCL.

IB.2.10. The bidder must have one office in Kolkata, West Bengal for providing necessary support. The details of such office needs to be provided by the selected bidder prior to placement of the LOA (Letter of Award)/ contract.

IB.3. Responsibility of Bidders:

IB.3.1. It shall be the sole responsibility of Bidders to determine and to satisfy themselves by such means as they consider necessary or desirable for all matters pertaining to this contract including, in particular, all factors that may affect the cost, duration and execution of the work.

IB.3.2. It must be understood and agreed that such factors have properly been investigated and considered while submitting the bid. Any claim, whatsoever, including those for financial adjustments to the contract, once awarded under these documents will not be entertained by WBSEDCL. Neither any change in time schedule of the contract nor any financial adjustments, arising thereof, shall be permitted by WBSEDCL, which are based on the lack of such clear information of its effect on the cost of the Contract to the Bidder..

IB.3.3. The bid should include all the information required in terms of the bid document. Submitted documents need to be specific as per requirements; irrelevant documents should not be uploaded by the bidder.

IB.3.4. The bidder shall bear all the costs associated with the preparation and

submission of bid and WBSEDCL in no case shall be responsible or liable for these costs, regardless of the conduct or outcome of the bidding process.

IB.3.5. In order to avoid any problem arising out of network error or server error, bidders are advised to submit the bid, well in advance of the last date and time of submission of the bid.

IB.3.6. One bidder can submit only one bid in response to this tender document. No bidder is allowed to submit two or more bids.

IB.4. General Guideline for e-Tendering:

Instruction/Guidelines for electronic submission of the tender have been mentioned below for assisting the bidders to participate in e-Tendering.

IB.4.1. Registration of Bidders :

Any bidder willing to take part in the process of e-Tendering will have to be enrolled & registered with the e-Procurement system, through logging on to https://wbtenders.gov.in.

IB.4.2. Digital Signature certificate (DSC):

Each bidder is required to obtain a Class-II or Class-III Digital Signature Certificate (DSC) for submission of tenders.

IB.4.3. The bidder can search and download NIeT & Tender Documents electronically from the https://wbtenders.gov.in website using the Digital Signature Certificate. This is the only mode of collection of Tender Documents.

IB.5. Signing of Bids:

IB.5.1. All documents uploaded/downloaded to/from the e-tendering web portal https://wbtenders.gov.in.need to be digitally signed through class-II or Class-III Digital Signature Certificate (DSC) for submission of tenders

IB.5.2. To be qualified for evaluation and finalization of contract, Bidder/ Bidders shall submit a written power of attorney, authorizing the signatory of the Bid to act on behalf of the Bidder in the form and manner which is acceptable by WBSEDCL.

IB.5.3. All the pages of the bid and where, entries/ amendments have been made, shall be signed by the person/persons signing the bid.

IB.5.4. The complete bid shall be without alterations, interlineations or erasers, except those to accord with instructions issued by WBSEDCL or as necessary to correct errors made by the bidders, in which case such corrections shall be initialed by the person/persons signing the bid. Bids not duly signed shall be treated as cancelled.

IB.6. Formation of cartel & penal Measures:

Any evidence of unfair trade practices, including overcharging, price fixing, cartelization etc. as defined in various statutes, will automatically disqualify the parties. Repeated occurrence of such evidence of above tenderers may also be viewed seriously by the WBSEDCL authority and penal measures as deemed fit would be imposed on such tenderers.

IB.7. Key Dates:

The schedule of publication, submission and opening of tender paper is furnished herein below:

SL No	Activity	Date & Time
1	Publishing Date	18.02.2026 at 14.00 Hrs.
2	Document Download start date	18.02.2026 at 14.00 Hrs.
3	Pre- Bid query submission last date and time	02.03.2026 at 14.00 Hrs.
4	Date of Pre-bid Discussion at, Vidyut Bhawan	16.03.2026 from 11.00 Hrs.
5	Bid submission start date	08.04.2026 at 16.00 Hrs.
6	Last date of physical submission of EMD, if not submitted online	22.04.2026 till 13.00 Hrs.
7	Bid submission end date	22.04.2026 till 14.00 Hrs.
8	Technical Bid opening date	28.04.2026 at 16.00 Hrs.
9	Financial Bid opening date	The date and time will be intimated after evaluation of Technical Proposal

If any 'Strike' or 'Holiday, falls on any of the scheduled date, then the next working day (between mentioned working hours) shall be considered as scheduled date and schedule time.

IB.8. Pre Bid Discussion:

IB.8.1. The bidder/OEM or its official representative is invited to attend pre-bid meeting which will take place at WBSEDCL Headquarters, Vidyut Bhawan, Kolkata, on the date and time specified in Clause **"Key Dates "** of Bid documents. The purpose of the meeting will be to clarify the exact scope of work, and any issues regarding the bidding documents in general and the technical specifications in particular which are raised at that stage.

IB.8.2. Only those queries which are submitted via mail by the Bidders (To - **network.itcell@wbsedcl.in**) within the timeline specified in the "Key Dates" shall be considered for discussion during the pre-bid meeting. Any queries, clarifications, or issues raised during the meeting that have not been submitted in advance may or may not be taken up, subject to availability of time and at the sole discretion of the Pre-Bid Committee .

IB.8.3. Non-attendance at the pre bid discussion will not be a cause for disqualification of the bidders.

IB.9. Clarification of Bidding Documents:

If there be any discrepancy or, obscurity in the meaning of any clauses of the Tender Documents or, if there be any query of the intending Bidder, the same may be clarified during the pre-bid discussion. The clarification given in the pre-bid discussion shall be final and binding on the Bidder and no further queries shall be entertained thereafter.

IB.10. Amendment / Addenda of Bidding Documents:

At any time, prior to the deadline of submission of Bid, WBSEDCL may, for any reason, modify the Bidding Documents by issuing Addendum / Amendments and the same will be uploaded on the website of WBSEDCL i.e. https://www.wbsedcl.in as well as website https://wbtenders.gov.in.

Bidders should keep a track of any such amendment and it will be assumed that the information contained therein has been taken into account by the bidder in its bid. if any, related to this NIeT on the WBSEDCL's website. The downloaded amendment/addenda is to be uploaded at the concerned location mentioned in clause "**Submission of Bid**".

In order to provide a reasonable time to prospective bidders for taking the amendment into account in preparing their bid, WBSEDCL may, at its discretion, extend the deadline for the submission of bids. In such cases, WBSEDCL will notify about the extended deadline to all the prospective bidders in writing through the e-tendering website (https://wbtenders.gov.in).

Such amendments, clarifications, etc., shall be binding on bidders and will be given due consideration by the Bidders while they submit their bids and also invariably submit such documents as mentioned in clause "**Submission of Bid**" part of the bid, which shall form an integral part of the contract.

WBSEDCL shall not have any obligation to inform the vendor through any other mode of communication.

IB.11. Language of the Bid:

The bid prepared by the bidder and all correspondences and documents relating to the bid, exchanged between the bidder and WBSEDCL, shall be written in English language.

IB.12. Period of validity of Bid:

Offered bids (both technical & price) shall remain valid for a period of 180 (One hundred eighty) days after the date set for opening of Bid.

Prior to the expiry of the original validity period, WBSEDCL may request extension in the period of validity to the selected bidder(s) only. Bidders agreeing to that request will not be required nor permitted to modify their respective bids, but will be required to extend the validity of their Bid Securities correspondingly. The provisions of clause "**Earnest Money [Bid Guarantee]"** regarding discharge and forfeiture of Bid Security shall continue to apply during the extended period of bid validity.

IB.13. Earnest Money [Bid Guarantee]:

IB.13.1. All bids must be accompanied with refundable earnest money, as "Bid Guarantee". The bid shall be considered non-responsive if the earnest money is not submitted along with the bid.

IB.13.2. The bidder shall select the tender to bid for and initiate payment of the EMD amounting to Rs. 45,00,000/- (Rupees Forty-Five Lakh only). Following payment options are available for paying EMD amount through online mode:

IB.13.2.1. E-payment can be made on the e-tender website https://wbtenders.gov.in through net-banking payment mode.

IB.13.2.2. RTGS/ NEFT Payment: On selection of RTGS / NEFT as the payment mode, the e-Procurement portal will show a pre-filled challan having the details to process RTGS/ NEFT transaction. The bidder will print the challan and use the pre- filled information to make RTGS / NEFT payment using his bank account. Once the payment is made, the bidder will come back to the e Procurement portal to continue the bidding process after expiry of a reasonable time to enable the RTGS/

NEFT process to be completed.

IB.13.2.3. **Submission of EMD through BG**: For submission of EMD in the form of BG issued by any Scheduled Bank of RBI, bidders will have to opt for EMD Exemption in e-tender portal and upload scanned copy of BG in the EMD exemption document upload section. Physical copy of BG shall be submitted at the office of tender inviting authority as per respective clauses of NIT. The Bank Guarantee shall be submitted as per format in ANNEXURE-III and shall remain valid initially for a period of 180 (one hundred eighty) days from the date of opening of bid document mentioned elsewhere in this NIT with a claim period of three (3) months thereafter.

IB.13.3. EMD amount shall be paid either in online mode or submitted through Bank Guarantee (BG) in full. Partial payment through online mode and remaining submission through BG is not allowed.

IB.13.4. **<u>General Instructions for EMD submission through Online:</u>**

IB.13.4.1. The bidder can deposit the EMD amount using net-banking mode through any bank available at e-payment gateway of e-tender site. Once Net-banking mode is opted for payment, the bidder will have to mandatorily pay through Net-banking facility.

IB.13.4.2. Status of NEFT/ RTGS payment through Challan for a bid may take time for bank settlement which is updated in 24 Hrs. (approx.). As such bidders opting to pay through NEFT/ RTGS mode shall make payment well before 24 Hrs. to avoid any complicacy.

IB.13.4.3. In case actual EMD amount as per NeIT is more than the one shown in E-tender Portal, bidders will have to opt for NEFT/ RTGS mode (challan mode). In that case the total actual EMD amount is to be paid only through NEFT/ RTGS mode (challan mode}.

IB.13.4.4. The bank account used for payment of EMD by the bidders shall be maintained operative until the completion of tendering process. All refunds will be made mandatorily to the Bank A/ c from which the payment of EMD has been initiated.

IB.13.5. **<u>General Instructions for EMD submission through BG:</u>**

IB.13.5.1. Earnest Money Deposit may be submitted through an irrevocable Bank Guarantee (BG) prepared in favor of WBSEDCL from any scheduled bank of RBI.

IB.13.5.2. Issue date of BG shall be after NIeT publication date.

IB.13.5.3. BG shall be submitted as per the format in ANNEXURE-III.

IB.13.5.4. WBSEDCL Bank Details for preparation of BG for EMD are as follows

i) WBSEDCL Bank Details for preparation of BG for EMD are as

follows:

Beneficiary Name: West Bengal State Electricity Distribution Company Limited (WBSEDCL)
Bank: PUNJAB NATIONAL BANK
Branch: MAYUKH BHAVAN Branch
A/C No: 1096202100000241
IFSC code: PUNB0109620

ii) In case of BG for EMD issued under SFMS Platform, the bank details are as follows:

Beneficiary Name: West Bengal State Electricity Distribution Company Limited (WBSEDCL)
Bank: PUNJAB NATIONAL BANK
Branch: MAYUKH BHAVAN Branch
A/C No: 1096250031639
IFSC code: PUNB0109620

IB.13.5.5. Original copy of BG for Earnest Money Deposit shall be submitted at the office address mentioned in clause **IB.28** of tender within the timeline given as per clause **"Key Dates"**. Scan copy of BG for EMD is also uploaded in e-tender site.

IB.13.5.6. Original BG i.r.o EMD shall be submitted in a sealed envelope at address as stated above within date and time as specified in the NIeT. If bidder fails to submit the original BG within the timeline specified in NIeT, the bid will not be considered for evaluation and hence rejected.

IB.13.5.7. The EMD in the form of Bank Guarantee (BG) shall be valid for a period of 180 (one hundred and eighty) days from the date of opening of bids with a claim period of three (3) months thereafter. The EMD shall be extended during the course of evaluation of bid, if requested by WBSEDCL.

IB.13.6. **Refund/Settlement of EMD Amount**:

IB.13.6.1. The bid guarantee of unsuccessful bidders, if submitted through e-payment or challan generated through e-tender website, will be refunded automatically, through an automated process, by NIC portal on receipt of updated status of any bid from WBSEDCL.

IB.13.6.2. The Bid Guarantee of unsuccessful bidders, if submitted through Bank Guarantee, will be returned against their written claim, to the Chief Engineer (IT Cell), WBSEDCL, giving the reference to the NIeT, date of tender, amount and mode of Earnest Money deposited – all in a complete form, after placement of an order on the successful bidder/bidders.

IB.13.6.3. For successful bid(s), EMD will be refunded from WBSEDCL authority

after completion of tendering process and submission of Performance Bank Guarantee as per respective clauses in NIeT. Successful bidder shall submit one letter addressed to Chief Engineer (IT Cell), WBSEDCL giving reference of NIeT, date of tender, amount, mode of earnest money deposited and details of Performance Guarantee for requesting refund/return of EMD amount or bank guarantee, as applicable. The selected bidder(s) may have to extend the validity of the Bid Guarantee till the Contract Performance Bank Guarantee is accepted by WBSEDCL.

IB.13.6.4. The bank account used for payment of EMD by the bidders shall be maintained operative until the completion of the tendering process. All refunds will be made mandatorily to the Bank A/c from which the payment of EMD has been initiated.

IB.13.6.5. For any queries related to payments and refunds, bidders will have to communicate: emd.eproc-wb@nic.in/sumi.chakraborty @ext.icicibank.com.

IB.13.7. Successful Bidder shall have to mandatorily create vendor id through WBSEDCL Web Portal Vendor Corner at www.wbsedcl.in, if not created earlier.

IB.13.8. No interest shall be payable by WBSEDCL on the above Bid Guarantee.

IB.13.9. The Bid Guarantee shall be forfeited for any of the following reasons:

IB.13.9.1. If during the period of bid validity, the bidder withdraws or modifies the bid in part or as a whole.

IB.13.9.2. If the successful Bidder/ Bidders fails/fail to accept the order unconditionally **as per "Acceptance of Order" clause** of bid document or fails/fail to furnish the contract performance guarantee as stipulated in PBG **clause** of bid document.

IB.13.9.3. If the successful bidder / bidders fails to extend the validity period of EMD as per **"Earnest Money" Clause** of bid document.

IB.13.9.4. If any cartel is formed by the bidder in their quotation.

IB.14. <u>Submission of Bid</u>:

<u>Bids shall be submitted as under</u> :

IB.14.1. Tender documents are to be submitted online through the website https://wbtenders.gov.in. All the documents uploaded by the Tender Inviting Authority form an integral part of the contract. Bidders are required to upload all the tender documents along with the other documents, as asked for, in the tender, through the above website within the stipulated date and time as given in the Tender.

IB.14.2. Tenders are to be submitted in two parts - one is **Technical Proposal** and the other is **Financial Proposal**.

IB.14.3. Pre-defined .xls format of Price bid under financial proposal is to be submitted at pre-defined folder named:BOQ. Price offered in any other shape or form or

any other Folder other than 'BOQ' will not be considered and concerned bid submitted by bidder will be liable for cancellation.

IB.14.4. The bidders shall carefully go through the documents and prepare the required documents and upload the scanned documents in Portable Document Format (PDF) to the portal in the designated locations of Technical Bid.

IB.14.5. The bidder needs to download the Forms / Annexures / BOQ, fill up the particulars in the designated Cell and upload the same in the designated location of Technical bid.

IB.14.6. The documents uploaded shall be virus scanned and digitally signed using the Digital Signature Certificate (DSC). Tenderers should take note of all the addendum/corrigendum related to the tender and upload the latest documents as part of the tender.

IB.14.7. Original copies of the uploaded documents may be submitted for physical verification if required by the Tender Inviting Authority at the time of technical evaluation.

IB.14.8. For each Item, the Bidder shall quote prices separately under:

Row 1 – Supply, Delivery & Installation-

The price shall include complete hardware (with all modules, accessories, power supplies, etc.), required software and licenses, integration, configuration, testing, and commissioning — ensuring a fully operational solution.

Row 2 – Five (5) Years Warranty & Maintenance Support

The price shall include comprehensive OEM warranty, FMS. software updates/upgrades, technical support, hardware replacement as per SLA, and any recurring license/subscription cost for the full 5-year period.

IB.14.9. Where a Bidder proposes a common hardware device or unified solution platform covering multiple functionalities under different BOQ Items, the pricing shall be structured as follows:

The complete hardware, software, and base license cost shall be quoted under one relevant BOQ Item (e.g., Item 1).

For the other related BOQ Item(s) (e.g., Item 2), only the applicable additional software and/or license cost shall be quoted.

IB.14.10. If the bidder is reusing the WBSEDCLs existing Cisco SD-WAN Type-B1 box, the Bidder shall quote only the required hardware/software upgrade and licensing cost in the BOQ for the item for full project period.

IB.14.11. Technical Proposal-(Part-1)

The Technical Proposal shall contain scanned copies and/or declarations in the following standardized formats in two covers / folder:

A. Statutory Cover: Fee/Pre qualification /Technical (All signed Copy is to submit) Under Statutory Cover/folder, there will be another four folders for submission of the technical documents.

I. To be submitted in **"Drafts"** folder- Earnest Money Deposit (EMD): If EMD is submitted through Bank Guarantee (BG), the following details are to be submitted:

Scanned copy of Bank Guarantee (BG) towards EMD in the format as prescribed in **Annexure III** of NIeT, in favour of WBSEDCL payable at Kolkata from any scheduled Bank of RBI. The issue date of BG shall be after NIeT publication date. This clause will be applicable only for cases where Earnest Money Deposit (EMD) has been submitted through BG.

II. To be submitted in **"Annexures"** folder-

General Annexures-

a) Bid Proposal (Vide **Annexure-I**).
b) Bid Details (Vide **Annexure-II**).
c) Earnest Money Deposit- Scanned copy BG (Vide **Annexure -III**) if EMD paid through BG.
d) Deviation Sheet (Vide **Annexure-IV**).
e) Blank Format of Proforma for bank guarantee for contract performance (Vide **Annexure-V**).
f) Format of the Bank Guarantee for additional performance security Deposit (Vide **Annexure-VI**).
g) Pre-BID Query Format(Vide **Annexure-VII**).
h) Blank BOQ (Vide **Annexure-VIII**).
i) Non Disclosure Agreement (Vide **Annexure-IX**).- To be submitted on normal paper during the technical evaluation stage of the tender. Upon placement of the Letter of Award (LOA)/during POC invitation, the same documents will be executed on non-judicial stamp paper as mentioned in Annexure.
j) Contract Agreement (**Vide Annexure-X**).-To be submitted on normal paper during the technical evaluation stage of the tender. Upon placement of the Letter of Award (LOA), the same documents will be executed on non-judicial stamp paper as mentioned in Annexure.
k) Mandatory Condition (Vide **Annexure-XI**).
l) Access security Policy **(Vide Annexure-XII).-** be submitted on normal paper during the technical evaluation stage of the tender. Upon placement of the Letter of Award (LOA), the same documents will be executed on non-judicial stamp paper as mentioned in Annexure.

Technical Annexures-

m) Network & Security Device – General Compliance Requirements (Vide **Annexure-T1**).
n) SD-WAN- Technical & Functional Requirements (Vide **Annexure-T2**).
o) SD-WAN Controller (Vide **Annexure-T3**).
p) 24-Port L2 Managed Switches (Vide **Annexure-T4**).
q) Centralized Switch-Controller – Technical & Functional Requirements (Vide **Annexure-T5**).
r) Specification for Indoor Access point (Wi-Fi) (Vide **Annexure-T6**).
s) Wireless Controller Specification (Vide **Annexure-T7**).
t) NAC, AAA and related solutions requirements (Vide **Annexure-T8**).
u) Reports, Dashboards & Analytics Compliance Sheet (Vide **Annexure-T9**).
v) Log Server Solution Requirements & Log Types Compliance Sheet(Vide **Annexure-T10**).
w) Virtual Lab Environment- Technical Annexure – Compliance Table (Vide **Annexure-T11**).
x) Technical Compliance Sheet: Rack for Network Equipment (Vide **Annexure-T12**).
y) Documentation Compliance (Vide **Annexure-T13**).
z) NOC Display, Monitoring PC & Accessories Technical Compliance Sheet (Vide **Annexure-T14**).

III. To be submitted in **"NIT"** folder-

a) Singed Notice Inviting e-Tender (NIeT)
b) Signed Addenda/Corrigenda: if published.

IV. To be submitted in **"Forms"** folder-

a) **Schedule of Bid**-The bidder needs to download the form for "Schedule of Bid" (Vide **Form-I**), fill up the particulars in the designated Cell and upload the same in the designated location of Technical Bid. Submission of incomplete "Schedule of Bids" will render the tender liable to summary rejection.

b) Check List (Vide **Form-II**).

c) Summary statement (Vide **Form-III**) of annual turnover for a period of the last three financial years i.e. for financial year 2022-23, 2023-24 & 2024-25 as per certified copy audit report in respect of bidders.

d) Proforma for undertaking to be submitted by the Bidders (Vide **Form-IV & VIII**).

e) Declaration of not being Blacklisted/Debarred/ Put on Holiday list (Vide **Form-V**).

f) Self-declaration by Proprietor of the Bidding Company for not being Blacklisted/Debarred/ Put on Holiday list (Vide **Form-VI**).

g) Declaration regarding no litigation against WBSEDCL (Vide **Form-VII**)

h) Format of Letter of Bid (Vide **Form-IX**)

Note: Bidders are to keep track of all the Addendum/Corrigendum issued with this particular tender and upload all the above digitally signed along with the NIeT.

B.Non-Statutory Cover (My Document): All Certificates are to be self-attested by the signing authority

a) Copy of CIN (Corporate Identification No) & Certificate of Incorporation.

b) Power of attorney for being signing authority of the bid.

c) Copy of Valid copy of PAN Card.

d) Copy of Valid Goods and Services Tax (GST) Registration certificate

e) Copy of GST returns for the years 2023-24 & 2024-25 are to be submitted by the bidder.

f) Copy of returns for IT filed during last three years i.e. for assessment years 2022-23, 2023-24 & 2024-25.

g) Audited financial statements for all three financial years (2022–23, 2023–24, and 2024–25)

Financial Info:

The bidder must have a minimum annual turnover of Rs. 100 Crore (Rupees One Hundred Crore only) in each of the financial years 2022–23, 2023–24, and 2024–25. Audited financial statements for all three financial years (2022–23, 2023–24, and 2024–25) must be submitted as supporting documents.

Credential:

Sl. No	Requisite Credential	Requisite Support document
1	The bidder should not have been included in any holiday listing from any Govt. organization across India in last three financial years, an undertaking in this regard shall be provided by the authorized signatory of the bidder. During the contract period if the undertaking submitted by the vendor is found to be false, the order issued on vendor shall be terminated with the forfeiture of the BG.	Self-Declaration from the Bidder with signature of authorized signatory of the bidder with company/ organization common seal.
2	The Bidder must have successfully implemented an SD-WAN solution with a minimum of 750 edge devices of the same OEM (SD-WAN software/hardware) in Single or Two LoA during the last Seven years from issuing date of tender.	Copy of order / agreement.
3	The bidder must have one office in Kolkata, West Bengal for providing necessary support. The details of such kolkata office needs to be provided by the selected bidder prior to placement of the LOA (Letter of Award)/ contract.	Self-declaration stating name and address of the office in Kolkata.

Note: Failure of submission of anyone of the above-mentioned documents may lead to rejection of the tender document.

IB.14.12. Financial Proposal-(Part-2)

The financial proposal needs to be submitted as per the pre-defined standardized formats in one folder named **"BOQ"** under the main folder "Finance". The bidder is to upload the downloaded predefined Price Bid (MS Excel format) only with filled-up amounts in specified fields. The bidder will not be allowed to upload any Techno-commercial terms and conditions in the 'Price Bid' offer/ BOQ. Any deviation taken in the Price part shall not be accepted.

The bidder is to quote the rate in the blank spaces marked for quoting rate in the BOQ.

Only downloaded copy of the BOQ is to be filled up, virus scanned, uploaded and digitally signed by the bidder. Any deviation in the format, content (Other than entry of the quoted price at the desired blank spaces) of the Price bid/BOQ will lead to rejection of the tender.

IB.14.13. Conditional and incomplete tenders are liable to summary rejection.

IB.14.14. No price preference will be allowed to any bidder based on the size of the industry or its geographic location. Co-operative Society will not be considered with separate status.

IB.15. Late Submission of Bid:

Bidder shall take all possible measures to submit the bid within the schedule date & time at specified location prescribed elsewhere in the bidding document. Late submission of bid for whatever reason shall not be accepted.

IB.16. Opening and evaluation of tender:

IB.16.1. Opening of technical proposal:

IB.16.1.1. Technical proposals will be opened by the Tender Inviting Authority or his authorized representative electronically from the website stated above, using their Digital Signature Certificate.

IB.16.1.2. Technical proposals for those tenderers whose original copies of BG towards EMD have been received will only be opened. Proposals corresponding to which original copy of BG towards EMD has not been received, will not be opened and will stand rejected.

IB.16.1.3. Cover (Folder) for Statutory Documents will be opened first and if found in order, Cover (Folder) for Non-statutory Documents will be opened. If there is any deficiency in the Statutory Documents, tender may be liable to be summarily rejected.

IB.16.1.4. Decrypted (transformed into readable formats) documents of the Statutory and Non-statutory Covers will be downloaded for the purpose of evaluation.

IB.16.1.5. The bidder shall not take any techno-commercial deviation from the stipulation of Bid document. If the bidder takes any techno-commercial deviation, his Bid may be liable for rejection.

IB.16.2. Evaluation of technical proposal:

IB.16.2.1. While evaluation, the Tender Inviting Authority or his authorized representative may summon of the bidders and seek clarification / information or additional documents or original hard copy of any of the documents already submitted and if these cannot be produced within the stipulated timeframe, their proposals will be liable for rejection.

IB.16.2.2. All Technical proposal documents as specified at the tender will be examined and assessed for the techno-commercial, performance and management capability of the bidder.

IB.16.2.3. The summary list of bidders, whose bids will be found techno-commercially eligible, will be uploaded in the web portals. Date of opening of financial bid will be intimated to the techno-commercially qualified bidders.

IB.16.3. Opening of financial proposal:

IB.16.3.1. Financial proposals submitted by the bidders in the prescribed BOQ format and declared techno-commercially eligible, will be opened electronically by the Tender Inviting Authority from the web portal stated above on the prescribed date.

IB.16.3.2. No deviation in any form in the price-bid sheet is acceptable.

IB.16.3.3. After opening of the financial proposal the preliminary summary result containing inter-alia, name of bidders and the rates quoted by them will be uploaded.

IB.16.3.4. The Tender Accepting Authority may ask any of the bidders to submit analysis to justify the rate quoted by that bidder.

IB.16.3.5. For any discrepancy in the amount of figures and words, the quoted amount in figure will prevail.

IB.16.4. Evaluation of financial proposal:

IB.16.4.1. Financial Evaluation of bid shall be made on the total price of all the items, clubbed together. This will however not encroach the right of WBSEDCL to go into further processes for item wise evaluation, if required. Total price shall be calculated on the basis of quantity indicated in the NIeT/BOQ.

IB.16.4.2. Price offer shall be submitted in the prescribed format only.

IB.16.4.3. No deviation in any form in the Price Bid Sheet is acceptable.

IB.17. Taxes, Duties and other levies:

GST and/or any other applicable tax as per law of land shall be paid extra. The GST/Tax will be paid, on production of original documentary evidence.

IB.18. Statutory Obligations:

Statutory obligations as per law of the land are to be complied.

IB.18.1. Compliance of Labour Laws: The bidder shall comply with all the statutory labour laws to protect the employees/workers engaged by them.

IB.18.2. Statutory obligations as per law of land are to be complied.

IB.19. Period of Contract:

Project period will be considered to be 5 years from the date of from the **date of Go-Live** (as mentioned in clause no. GCC.1. Project Timeline).

WBSEDCL may increase the period of contract for another 2 (Two) years in a sequel of 1(One) year each depending upon the performance during the project period of the successful bidder at the same terms and conditions as in the Letter of Award (LOA) placed on successful bidder and which shall be accepted by the bidder without imposing any conditions.

IB.20. Execution Period:

The basic consideration and the essence of the contract shall be in strict adherence to the time schedule as it will be specified in the LOI (Letter of Intent)/LOA (Letter of Award) to be issued from WBSEDCL. The entire project activity mentioned in clause no. **GCC.1. Project Timeline**.

IB.21. Issuance of LOA :

WBSEDCL will award the contract to the successful bidder whose bid has been determined to substantially responsive and has been determined the lowest evaluated bid, provided further that the bidder is determined to be qualified to perform the contract satisfactorily. WBSEDCL shall be the sole judge in this regard.

IB.22. Acceptance of LOI/LOA:

The successful bidder shall submit written unconditional acceptance of LOI/LOA within 15 (Fifteen) days from date of issuance of the same. Submission of conditional acceptance of

LOI/LOA shall be treated as non-compliance of this clause. In case of non-compliance, WBSEDCL reserves the right to cancel the LOI/LOA placed on you.

IB.23. Right to reject Bids:

WBSEDCL reserves the right to accept or reject any bid and to annul the bidding process and reject all bids at any time prior to award of Contract, without thereby incurring any liability to the affected bidder or bidders or any obligation to inform the affected bidder or bidders the reason for WBSEDCL's action.

IB.24. Conflict of Interest:

The Bidder shall not have a Conflict of Interest that may affect the Tendering Process. Any Bidder found to have a Conflict of Interest as per the following reasons, shall be disqualified. In the event of disqualification, the Bid Security of the bidder shall be forfeited for the time; cost & effort of the Authority including consideration of such Bidder's Proposal, without prejudice to any other right or remedy that may be available to the Authority hereunder or otherwise

Any bidder will be found to have a conflict of interest if his near relative is posted as an employee/ officer in any capacity in WBSEDCL, who is associated with the Tender inviting Authority or vice versa.

Any bidder will be found to have a conflict of interest if any employee of the bidding firm/company has or develops a financial or other interest with any employee / officer of WBSEDCL associated with the Tender inviting Authority during the execution of the Contract or vice versa.

Any bidder has a relationship with another bidder/bidders directly or through common third parties that puts them in a position to have access to each other's information about or to influence the tendering processes of either or each of the other bidder, will be found to have conflict of interest.

IB.25. Settlement of Disputes:

In case of any dispute arising out the contract, the same should be settled through meeting process between the WBSEDCL and the contracting agency at the appropriate level. The unsettled/unresolved issues/disputes shall be adjudicated by the competent court within the jurisdiction of Hon'ble High Court, Calcutta, if approached by either party.

IB.26. Mandatory Condition:

The bidder shall provide documentary evidence satisfactory & acceptable to WBSEDCL to establish that they have the requisite credential, capability and experience to handle the contract and meet requirements of all the Mandatory Conditions indicated in **Annexure-XI.**

IB.27. Clarification of Bids:

To assist in the examination, evaluation and comparison of bids, WBSEDCL may ask the bidder individually for clarifications of his bid at the appropriate stage of evaluation. The request for clarification and the response thereof shall be in writing but no change in the price or substance of the bid shall be sought, offered or permitted.

IB.28. Communication:

For communicating with WBSEDCL, for this job may use the following modes. Mail-id-network.itcell@wbsedcl.in.

Communication for letter: Chief Engineer, IT Cell, Vidyut Bhavan,3rd Floor, D Block, Block-DJ, Sec-II, Kolkata-700091

IB.29. <u>Representative of Vendor</u>:

IB.29.1. Bidder have to nominate one personnel exclusively for this project from commencement to completion as a Nodal Officer to be stationed at Kolkata, with whom WBSEDCL will contact on all matters related to this order.

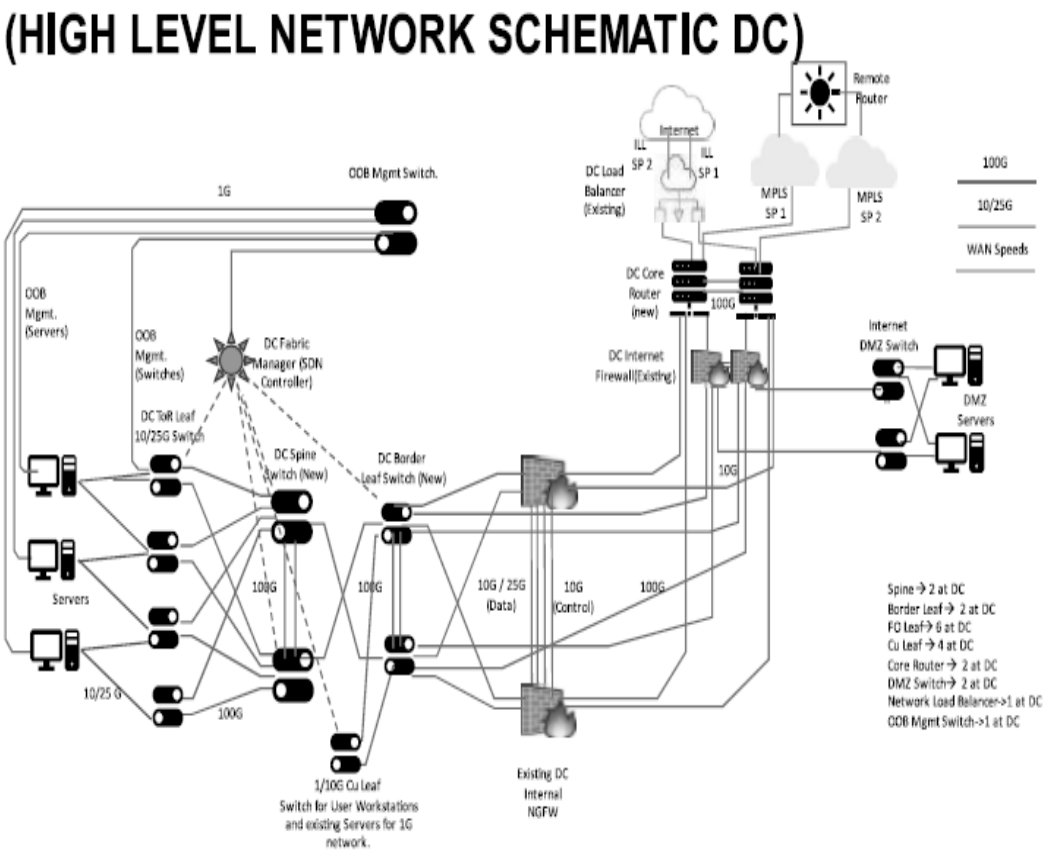
IB.29.2. Bidder have to specifically furnish to WBSEDCL, the name, designation, Telephone no. including mobile no., email address of such person.

IB.29.3. Bidder have to allocate personnel at WBSEDCL office as assigned by controlling officer of this project for monitoring.

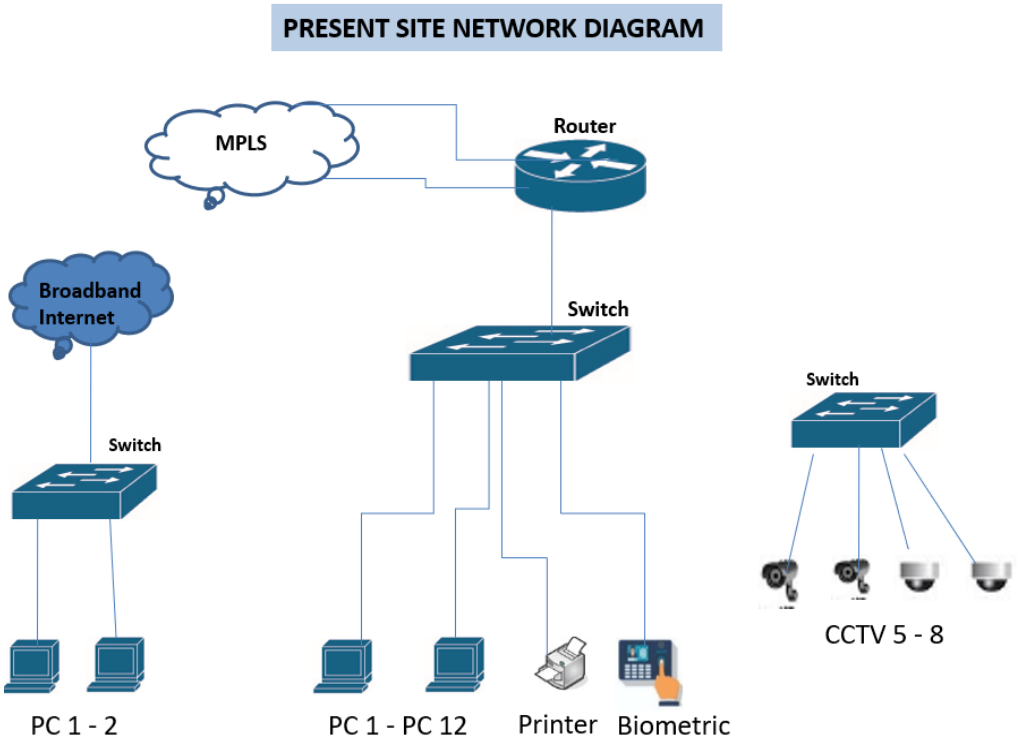
SECTION: II
Scope of Work [SW]

1. WBSEDCL proposes to upgrade its network infrastructure to achieve enhanced security, centralized management, and improved visibility through SD-WAN, managed switches, enterprise Wi-Fi, NAC-AAA, centralized logging, reporting, and analytics solutions, along with other related network and IT infrastructure solutions. The selected bidder shall be responsible for the end-to-end supply, installation, configuration, testing, commissioning, and warranty support of all required hardware, software, licenses, firmware, and associated components All activities shall be carried out in compliance with the terms and conditions set forth in this RFP document and any subsequent corrigenda or pre-bid clarifications issued by WBSEDCL.

2. Present network diagrams-The central locations—Data Centre (DC), Disaster Recovery Centre (DR), Vidyut Bhawan (Headquarters), and ALDC are connected through dual, high-speed MPLS and Internet Leased Line (ILL) links with built-in redundancy and automatic failover mechanisms, ensuring high availability, resilience, and reliable connectivity for critical operations. The DC and DR are equipped with full-fledged data center–grade infrastructure, while HQ and ALDC are provisioned with core network architecture comprising redundant core switches, high-capacity links, and industry-standard resiliency controls, aligned with best practices. An overview of the existing Data Centre network architecture is illustrated in the below diagram.



Site office network overview: Site offices are provisioned with MPLS connectivity for core business applications, along with separate broadband internet connections or ILL for general and ancillary usage. An overview diagram is as below:



3. The following devices and solutions shall be supplied, deployed, licensed, integrated, and supported under this Network Upgradation Project, in accordance with the respective Technical Annexures:
    1. SD-WAN boxes (5 types) – 750 nos.- Annexure T-2.
    2. SD-WAN Controller – 2 nos.- Annexure T-3.
    3. Managed Network Switch (Layer-2, 24 port) – 800 nos.- Annexure T-4.
    4. Managed Switch Controller – 2 nos.-Annexure T-5.
    5. Wi-Fi Access Points – 24 nos.- Annexure T-6.
    6. Wi-Fi Controller – 1 no.- Annexure T-7.
    7. Network Access Controller & AAA – 2 nos.- Annexure T-8.
    8. Reporting, Dashboard & Analytics – 2 nos.-Annexure T-9.
    9. Log Server Solution – 2 nos.- Annexure T-10.
    10. Client VPN (ZTNA) – 200 nos. concurrent users. - In Annexure-2.
    11. Virtual network lab set up solution -1 nos.- Annexure T-11
    12. Network rack- 100 nos. (Approx.)- Annexure T-12
    13. NOC-Display and PC set up solution. -5 nos.- Annexure T-13

4. General and Documentation Compliance: Annexure T-1 defines the General Technical, Security, Compliance, and Operational Requirements, which shall be applicable uniformly to most devices, solutions, and services under this project (details in Annexure T-1). Annexure T-14 defines the Documentation Requirements, including design documents, configuration details, SOPs, manuals, and lifecycle documentation, and shall be applicable across the entire project scope.

5. Solution Architecture & Interoperability (All Devices): The proposed solutions may be delivered as (a) a single integrated platform or (b) multiple dedicated devices/modules. From one or more OEMs provided that every component fully meets the functional, security and performance requirements that have been put in this tender and operates in tight coordination and bidirectional integration without compromising any feature.

6. All major components must be on-premises, support high availability across DC/DR (Active-Active or Active-Standby with state synchronization), and interoperate seamlessly with each other and with the WBSEDCL's network and security stack, including but not limited to SIEM, Threat Intel servers, DNS, SDN switch networks, existing core switches and LAN network switches, EDR, and NMS, as well as planned future network security systems.

7. Delivery, installation, preventive maintenance services, and technical support shall be provided by the bidder across the State of West Bengal in all WBSEDCL offices. The approximate list of Customer Care Centre (CCC) office locations is available on our website under: About Us → Contact → Customer Care Centre**.** If a detailed and complete list of locations is required, bidders may request the same through the email ID provided later in this RFP (Tender clause- "Communication") .

8. Architecture Considerations (to be factored by Bidders):

9. WBSEDCL currently has two external firewalls, two internal firewalls and two load balancers at both the DC and DR locations, operating in either active–active or active–passive mode as per requirement. These devices are under active support and shall be incorporated into the upgraded SD-WAN architecture. The placement, logical design, and integration approach shall be finalized jointly by the Bidder and the WBSEDCL's technical team. Any additional details required may be obtained by email request (Tender clause- "Communication") .

    a. WBSEDCL has different types of LAN networks SDN, traditional LAN, Core switches, L2 or L3 switches etc. at different central locations and site offices. Any additional details required may be obtained as per process mentioned in this RFP

    b. WBSEDCL has four SD-WAN–capable Cisco boxes (Type B1 boxes, as detailed in the SD-WAN Box Annexure), with two deployed at the Data Centre (DC) and two at the Disaster Recovery Centre (DR). These devices were recently procured as part of the DC/DR upgradation and are available for integration as part of the proposed SD-WAN implementation, with the objective of optimal utilization of existing investments. It is clarified that no SD-WAN controller, orchestrator, or centralized management platform has been procured as part of this deployment, and only the above-mentioned edge devices are available for reuse.

        1) The Bidder is expected to leverage these existing devices, either directly or through additional devices, middleware, or equivalent solutions, as required, to ensure seamless integration and interoperability with the proposed solution under this project.
        2) If the Bidder proposes an SD-WAN controller or orchestration platform from an OEM other than Cisco, then all additional edge devices, reconfiguration with new SDWAN related OS or configurations, integration with Controller, licenses, gateways, middleware, or any other components required to achieve full compatibility and integration shall be supplied by the Bidder as part of the solution.

3) Conversely, if the Bidder proposes to use Cisco SD-WAN controllers, then the existing Cisco Type-B1 boxes made available by the WBSEDCL must be upgraded—including throughput, licensing, image/software version, and any other feature support—to meet all technical and functional requirements as specified in this RFP and the Technical Annexure for entire project period. Full OEM-supported upgrades and compliances must be ensured.

4) Any solution proposed must ensure full functionality as per SD-WAN feature and technical requirements mentioned in the RFP.

5) These boxes (or the combined box + additional device setup) must offer a minimum full warranty support for throughout project period and match all technical specifications laid out for SD-WAN edge devices and to be managed by bidder.

6) Further details or technical specifications of these boxes, warranty coverages shall be shared only with intended bidders on a formal request, respecting security protocols as mentioned in this RFP earlier.

10. The current network traffic patterns and service dependencies of the WBSEDCL must remain unaffected during and after the SD-WAN deployment. The upgraded network must offer equal or improved performance, stability, and security across all traffic types. The key traffic flows are as follows (but not limited to):

a. Internal Application (Intranet) Traffic: Multiple core applications are hosted at the WBSEDCL's DC and DRC sites. These are accessed by field and remote offices via the existing internal MPLS VPN network. This intranet application access must continue uninterrupted and with improved latency and availability post-upgrade.

b. Internet and cloud traffic: WBSEDCL deliver various citizen-facing and employee **services** via the internet hosted at our data center and cloud. Additionally, access to cloud-hosted applications and other government platforms is also done through the internet (and also using dedicated MPLS for some scenarios). SD-WAN must ensure secure, policy-based access to these services with visibility and control mechanisms in place.

c. Video Conference traffic: Regular video conferencing sessions are held between HQ, DC/DR, and site offices over intranet, internet, or State Government LAN/MPLS networks. Various VC endpoints and software clients are in use. The SD-WAN network must support seamless video conferencing with adequate bandwidth prioritization (QoS), jitter control, and fallback mechanisms.

d. IVRS and Telephony Traffic- WBSEDCL uses SIP or PRI-based IVRS systems for receiving consumer calls and complaints. Additionally, IP phones and unified communication tools are deployed at various offices. The SD-WAN solution must support reliable voice call routing and signaling traffic for both internal and external communication.

e. Surveillance, Biometric & Access Control Traffic- Devices such as CCTV cameras, biometric attendance systems, door access controls, and related peripherals are

deployed across field offices and critical sites. The SD-WAN network must ensure these systems remain continuously connected to central monitoring systems with low latency and lossless video streaming support, wherever applicable.

11. The proposed solution has many components related to WBSEDCL Datacenter, Network and Security. The Service Provider must ensure that every installation, renewal, upgrade, or new purchase has been verified by understanding existing Licenses, configuration, network connectivity, Application / Service Integration and Security and Policy requirements of the WBSEDCL. It will be the Service Provider's ultimate responsibility to hand over the Modernized Infrastructure in proper working condition as per WBSEDCL requirements and compliant with WBSEDCL and Government of India IT Security policy.

12. The bidder shall design, configure, and implement the network architecture to ensure secure and efficient connectivity from all site locations to the WBSEDCL's Data Center (DC), Disaster Recovery Center (DR), and approved Cloud DC/DR, as per operational requirements. Bidder must deploy experienced network architect for the same.

13. The design shall define traffic flow, routing, segmentation, and security policies across sites, DC/DR, and cloud environments, ensuring high availability, performance, and compliance with WBSEDCL standards. Also, hybrid mode of working plan to be defined with traditional network and upgraded SDWAN network sites both working together.

14. The network architecture may be modified during the project period to meet evolving WBSEDCL's requirements, and the Service Provider shall implement such changes in accordance with approved requirements and change-management procedures.

15. The bidder must conduct a comprehensive survey of the existing network architecture at DC, DR, VB, ALDC and site offices. Develop a detailed design, integration, and migration plan for all offices. The same shall be submitted as per Project Timeline. Approval shall be obtained from WBSEDCL before initiating migration to the upgraded network.

16. Any additional details or technical information required for bid preparation—relating to internal network architecture, devices, or infrastructure for any location—shall be shared only with the intended participating Bidders, upon formal request via mail (Tender clause- "Communication"). Such information will be provided strictly on a need-to-know basis, in compliance with the WBSEDCL's confidentiality, security, and data protection policies. Information potentially to be shared on a need-to-know basis.

17. Design and Migration Plan- Based on the assessment, the vendor shall prepare and submit a detailed end-to-end network design on virtual lab, integration blueprint, and phased migration plan for transitioning from the existing dual-MPLS setup to the proposed SD-WAN-based architecture without affecting official work. The design must also include the planned placement, logical integration, coordinated working, and interaction of the following network and security components, duly considering the existing DC/DR and site infrastructure architecture:

    a. SD-WAN edge devices and controller/orchestrator

    b. Managed switches and controller

    c. Network Access Control (NAC) and AAA systems

d. Centralized logging, reporting, and analytics systems

e. Wi-Fi access points and controller

f. Existing firewalls, DNS, DHCP architecture, load balancers, application servers, reverse proxy servers, and related DC/DR and site components

18. Upon approval of the design and migration plan, the vendor shall begin execution in a phased manner –as per Project Timeline, ensuring minimal disruption to ongoing services. The vendor must ensure compatibility of SD-WAN with hybrid deployments at designated sites, where both MPLS and Internet circuits may be used concurrently.

19. Consortium not allowed- The bidder must participate **individually**. Consortium bids, joint ventures, sub-contracting of core scope, or any form of alliance for the purpose of meeting eligibility or technical requirements are not permitted under this project. All responsibilities—including supply, implementation, integration, support, and warranty—shall be fulfilled directly by the bidder.

20. For working together in shared network infrastructure components (e.g., SD-WAN devices, firewalls, switches, NAC, IPAM systems) which may be co-managed or require interfacing between multiple administrative domains, and to ensure smooth coordination, security integrity, and uninterrupted operations during the implementation and lifecycle management of the SD-WAN and associated network infrastructure. The successful Bidder shall work in coordination with the WBSEDCL and Data Centre SI to ensure the following:

    a. Seamless Device Sharing Protocols – Procedures for secure configuration and management of shared devices without conflict or override of existing settings critical to other services.

    b. Access Control and Audit Compliance – Role-based access to devices shall be mutually agreed upon and implemented, with complete traceability and audit logs maintained in compliance with ISO 27001 and CERT-In guidelines.

    c. Change Management and Coordination – Any device-level changes, upgrades, patching, or incident responses must be coordinated through a jointly defined and documented Change Control Process involving all three parties.

    d. Security and Ethical Operations – All parties shall adhere to best practices for secure administration, including non-repudiation of actions, no unauthorized configuration or credential changes, and immediate reporting of anomalies or breaches.

    e. Non-Disruptive Workflows – The operational and security activities of one party must not impact the availability or performance of services managed by the others. Mechanisms for maintenance windows, fallback, and rollback procedures must be mutually defined.

21. Delivery at Site, DC/DR Requirements-

    a. Cables, Power, and Accessories -The bidder shall be responsible for supplying all necessary power cables, power cords, fiber patch cords, compatible SFP modules, connectors, data cables, check nuts, and any other required accessories for the

installation and commissioning of devices across all site offices, Data Centre (DC), and Disaster Recovery (DR) locations. WBSEDCL shall only provide rack space and power availability at designated points.

b. Delivery Schedule & Planning: As per project timeline delivery instruction, The Bidder shall submit a detailed, location-wise delivery schedule covering all sites, DC, and DR, clearly indicating proposed delivery dates and phases. Delivery shall commence only after review and go ahead by WBSEDCL. All deliveries must be executed during working days and official working hours of WBSEDCL unless otherwise approved. An incident as per WBSEDCL format to be raised by L2 personnel (in coordination with L1 personnel there and site office in charge) and approved scan copy of delivery acceptance sheet by site in charge to be uploaded in WBSEDCL incident management system. The original hard copy shall be submitted along with the corresponding bill. Liquidated Damages (LD), if applicable, shall be calculated based on the incident date recorded in the system.

c. Installation Completion & Documentation - Mentioned in details latter Scope of Work Point 59.

d. Delivery Handling and Site Access- All device deliveries, unloading, unpacking, and staging at respective sites (including DC, DR, and remote offices) shall be managed by the bidder.

1) Bidder personnel must carry valid ID cards and obtain prior access approval from the WBSEDCL for entry into offices and WBSEDCL area.

2) For access to critical infrastructure locations prior written approval must be obtained from the WBSEDCL's authorized representative.

3) WBSEDCL reserves the right to deny access in the absence of proper identification or security clearance.

4) The bidder shall engage its personnel's and on-site OEM-certified professionals to deploy and configure all components at the Data Centre (DC) and Disaster Recovery (DR) sites as per the technical specifications outlined in this RFP. Use of VPN or remote connectivity is strictly prohibited during deployment, configuration activities or maintenance of this project. However, remote access may be permitted only in exceptional or emergency situations, and strictly subject to prior written approval from the WBSEDCL's designated authority.

22. Installation & Commissioning Requirements-

a. **Device Installation & Configuration**

1) Install and configure all devices, agents, servers, and controllers that fall within the scope of this project.

2) Validate power availability, cabling, rack placement, firmware/software versions, controller onboarding, routing, tunnel status, security policies, and overall device health.

3) Integrate all relevant components with the WBSEDCL's AD/LDAP/LDAPS, DNS, NTP, SIEM, NMS, and other required solutions, and apply baseline access and security policies as instructed by WBSEDCL.

b. **Endpoint Readiness – NAC & TLS/SSL**

1) Ensure installation or verification of the NAC Agent and the TLS/SSL Inspection Certificate on all functional PCs/laptops of the WBSEDCL by visiting site offices.

2) Prepare a site-wise and consolidated summary report indicating total PCs, number of PCs with NAC installed, number with TLS/SSL installed, and reasons for any pending installations. Reasons attributable to WBSEDCL's issues may be exempted after review by WBSEDCL's team; all vendor-related gaps shall be addressed and resolved by the Vendor.

c. Documentation & Installation Completion Certificate

1) Prepare a Site Installation & Commissioning Certificate for each location, signed by the Site In-charge.

2) The certificate shall include SD-WAN and switch serial numbers, confirmation of installation and configuration, and summary of NAC/TLS status.

3) Include any observations or pending items relevant to the installation.

d. **Incident Registration & Commissioning Confirmation**

1) The Bidder's L1 engineer shall email the signed commissioning certificate, the summary report, and the required photographs (one full rack view showing the SD-WAN device and switch in running condition, and one photograph clearly showing the serial numbers of the SD-WAN device and switch) to the designated L2 onsite personnel.

2) The L2 engineer shall raise an incident in WBSEDCL's incident management tool under the Installation/Commissioning category, providing complete site/location details and uploading the scanned documents and photographs submitted by the L1 engineer.

3) The incident creation date shall be treated as the official commissioning date for the particular site, subject to successful completion of all installation activities and submission of all required documents, reports, and photographs.

23. Hybrid Mode and Business Continuity- The vendor must ensure uninterrupted business operations and service availability across sites that continue to run on traditional dual-MPLS setups as well as those upgraded to SD-WAN. The network design and implementation must support hybrid mode deployment, where both MPLS and Internet-based SD-WAN connections may coexist at different sites or within the same site during transition.

a. The DC, DR, and VB locations must be capable of handling both traditional MPLS traffic and SD-WAN traffic simultaneously until the SD-WAN solution is fully deployed, tested, and stabilized across all sites. Only after the WBSEDCL issues confirmation of successful end-to-end deployment shall all traffic be fully transitioned to the SD-WAN network.

b. The vendor must submit a hybrid working strategy and failover/resiliency plan as part of the migration design.

c. The SD-WAN solution should support dynamic path selection, intelligent routing, and policy-based traffic handling between MPLS and internet circuits.

d. Centralized monitoring, control, and troubleshooting capabilities must be retained across both traditional and SD-WAN environments.

e. The Bidder shall ensure that the migration from the existing traditional MPLS router infrastructure to the new SD-WAN solution is carried out in a parallel, seamless, and non-disruptive manner. During the transition phase, both traditional MPLS circuits

and SD-WAN links must remain fully operational to avoid any interruption to official work or critical services.

f. Any additional devices, servers, modules, cables, accessories, or temporary equipment required to support the dual-running (MPLS + SD-WAN) setup during the migration period shall be provisioned by the Bidder at no extra cost to the WBSEDCL.

g. The Bidder shall ensure that all migration activities are executed with proper planning, maintaining network availability and ensuring that official work, applications, connectivity, and service delivery remain unaffected throughout the transition period.

24. Licensing and Authenticity Compliance-

a. All software, hardware, licenses, and firmware supplied under this project must be genuine, original, and legally sourced from the respective OEMs or authorized distributors. The bidder shall ensure that no pirated, counterfeit, cracked, or unauthorized versions are deployed or used at any stage of the project.

b. Use of open-source software for any core functional component of the solution is not permitted, unless explicitly approved in writing by WBSEDCL.

c. The bidder shall be fully responsible and accountable for the legality and authenticity of all components supplied, and shall provide valid license certificates and documentation wherever applicable.

d. In case of any violation or detection of counterfeit items, WBSEDCL reserves the right to take legal and contractual action, including immediate disqualification or termination.

25. Post implementation support, Maintenance and Upgrades-

a. The bidder shall provide end-to-end, on-site, comprehensive support/maintenance and warranty for all the devices and solutions in this project—**for a period of five (5) years** from **Go-Live date (start date of warranty /maintenance period)** as in Project Timeline.

1) The warranty must include back-to-back support from the respective OEMs for all hardware and software components. Need to submit Manufacturer Authorization Form (MAF) from respective OEM.

2) It shall cover all defects arising from faulty design, materials, workmanship, or media failure.

3) The bidder shall ensure free replacement of defective hardware, reinstallation of software/firmware, patch deployment, and necessary upgrades to maintain performance, security, and compliance.

4) This comprehensive support shall include both preventive and corrective maintenance for all covered devices and systems.

b. During the warranty period, the bidder shall offer comprehensive support for all supplied hardware, operating software, firmware, and related components at no additional cost to WBSEDCL. This includes ensuring that all components remain compliant with the defined acceptance parameters. The bidder shall bear all costs related to preventive and corrective maintenance, labor, spares, security compliance,

and transportation to and from the site for repair or replacement of any component (hardware/equipment/software or subcomponents) that proves defective under normal usage.

c. The bidder shall ensure the availability of professionally qualified personnel for on-site support to perform daily operational maintenance as per OEM guidelines. This includes firmware/software reloading, security compliance checks, patch management, system recovery in the event of crashes or malfunctions, fine-tuning of configurations, system monitoring, log verification, and general upkeep of all network devices deployed under this project.

d. In the event of any failure, disruption, or anomaly, the bidder shall be responsible for conducting a Root Cause Analysis (RCA**)** and submitting a detailed report in the format prescribed by WBSEDCL, including corrective and preventive actions (CAPA) to avoid recurrence.

e. On-site comprehensive warranty shall include the free replacement of defective parts, kits, and components, along with the complete resolution of any issues affecting the deployed solution.

f. Support services must be on-site and comprehensive in nature, with active back-to-back support arrangements in place with all relevant OEMs. The bidder shall warrant all supplied products against defects arising from faulty design, material, or workmanship. Support must also cover pre-installed operating systems and software components for the duration of the hardware warranty.

g. The bidder shall ensure that all critical, security, and firmware/software patches related to the deployed components—including SD-WAN devices, switches , SDWAN & Switch controllers, DHCP/IPAM systems, and analytics tools—are evaluated, tested in a controlled environment, and deployed in a timely manner during the support period.
Patch deployment shall follow a defined change management process approved by WBSEDCL to ensure system stability, security compliance, and minimal disruption to services.

26. Documentation Standards and Compliance -The bidder shall prepare and submit all project documentation as defined in the Technical Annexures for Documentation, including but not limited to design documents, configuration records, operational SOPs, administrative access details, and the final consolidated master documentation package etc.

a. All documents shall be delivered in both editable format and duly signed PDF, and must conform to ISO/IEC 27001:2022 or latest documentation standards, including proper versioning, authorship, approval metadata, change history, controlled distribution, and mandatory updates following any configuration, device, or user change.

b. **Go-Live (start of warranty and maintenance period) shall be permitted only after** WBSEDCL **has received, verified, and approved all required documents**.

c. Periodic submission and updating of documents as per Technical Annexures for Documentation, if not done SLA will be applicable as mentioned in SLA part.

27. Audit, VAPT & Security Event Compliance Requirements-The Bidder shall fully support all audit-related activities—including internal audits, external audits, ISO/IEC 27001:2022 or latest audits, and VAPT exercises—conducted by the WBSEDCL or any authorized agency.

28. The bidder and the deployed L2 onsite personnel, along with L3 support teams, shall provide all required logs, configuration details, reports, justifications, and responses within the timelines defined by the WBSEDCL. Any gaps, observations, or non-conformities identified during audit/VAPT activities must be promptly addressed by the bidder through corrective and preventive actions, with closure reports submitted in the WBSEDCL-approved format.

29. In case of any IT security alerts, events, or incidents reported by the WBSEDCL, CERT-In, MeitY, or other Government Security Agencies, the bidder shall provide full cooperation, including timely information sharing, technical support, forensic inputs (where applicable), and RCA reporting. All responses, artefacts, and technical actions must comply with the WBSEDCL's security standards, incident handling guidelines, and regulatory directives issued by competent authorities.

30. **Change Management-**Bidder must follow the WBSEDCL's formal Change Management Policy and must conform to ISO/IEC 27001:2022 or latest standards.
    a. The bidder must raise Change Requests (CRs) with complete details: impact analysis, risk assessment, rollback plan, and deployment methodology.
    b. All changes shall be executed only during approved maintenance windows or scheduled change periods.
    c. Provide comprehensive change-closure reports with evidence, activity logs, and compliance confirmations.

31. WBSEDCL's **Incident Reporting System** must be used for recording, tracking, and closing all incidents related to devices and solutions in this project. All operational, performance, security, or patch-related failures must be logged as incidents. The bidder shall perform comprehensive RCA (Root Cause Analysis) for each incident, including technical cause, impact, and corrective & preventive actions. RCA reports shall be submitted in the WBSEDCL -approved format and within defined timelines.

32. Patch Management and Testing Process- The bidder shall design, implement, and maintain a **comprehensive Patch & Firmware Management Process** for all project components (SD-WAN, switches, NAC, controllers, servers, NMS, security tools). The procedure shall comply with **ISO 27001:2022 or latest** , WBSEDCL audit requirements, and OEM best practices.
    a. **Controlled Patch Testing Environment**
        1) Establish a closed, isolated test environment using any SD-WAN device, managed switch provisioned under this project, and a dedicated test PC.
        2) Validate all firmware, OS images, and patches for stability, interoperability, and security.
        3) Maintain test logs, results, and approvals before rollout.
    b. **Patch Rollout – SD-WAN Devices & Switches**
        1) Apply patches first to a selected pilot group of site offices.
        2) After pilot success, roll out patches in phases to all sites.
        3) Maintain automated backups, pre/post-health checks, and rollback readiness.
    c. **Patch Rollout – NAC, Controllers, NMS & Servers**

1) Follow DR-first deployment and validate patches on DR before DC.
2) Use rolling upgrade methods for clustered systems.
3) Prioritize critical and security patches as per OEM advisories.

d. **Patch Classification & Governance**
   1) Classify patches into critical, security, functional, feature, and major updates.
   2) The bidder shall be fully responsible for evaluating, approving, coordinating, and deploying all patches and firmware updates in consultation with the respective OEMs
   3) Track vulnerabilities and ensure timely mitigation. The bidder shall proactively coordinate with OEMs to review advisories, vulnerability bulletins, and recommended hotfixes, and shall ensure the systems remain on supported and secure versions.

e. The bidder shall maintain a Patch Management Register in Excel or equivalent for each device type and must be shared with WBSEDCL as per requirement. Each sheet shall include, at minimum, the following columns: Device Make & Model, Serial Number/Asset ID, Site Name/Location, IP Address/Hostname, Environment (Production/DR/Test), Current Firmware/OS Version, Current Patch Level, Last Patch Date, Patch Type((Security / Critical / Functional / Major Upgrade), Support Status (Supported/End-of-Support/Needs Upgrade), Patch Description, Deployment Date, Deployed by, and a Remarks column to record rollback details, issues observed, and any other relevant notes.

f. Logs must be maintained for audit purposes as per ISO 27001:2022 and CERT-In requirements. Incident reporting also as per CERT-In guidelines.

33. Training- The vendor shall provide structured, hands-on training and comprehensive knowledge transfer sessions to the WBSEDCL's team (5 members) , with a strong focus on operating, managing, and troubleshooting the deployed infrastructure. The training must be practical, device-specific, and aligned with day-to-day operational needs, using the respective GUI tools, controllers, and dashboards.

a. The complete training program shall be delivered **before submission of the 1st Service/Maintenance Bill of the first Half year.** WBSEDCL shall not be liable to process or release the 1st half year service/maintenance bill unless the vendor successfully completes all mandated training sessions and submits an official Training Completion Certificate, duly signed by authorized representatives of the WBSEDCL.

b. Training must be delivered primarily **on-site with the physical presence of trainers**. Online support may be used only as an exception, such as for remote OEM expertise or troubleshooting assistance. However, it must not replace on-site sessions and should be kept to a minimum. The vendor must ensure that logistical and operational arrangements are made to facilitate full in-person training delivery for all essential modules.

c. Trainers must be OEM-authorized or vendor-certified, with actual network designing or deployment experience.

d. To ensure that the WBSEDCL's operational responsibilities are not impacted during the training period, the training program shall be conducted in half-day sessions of 3.5 hours per day. Training sessions may be scheduled either in the morning or afternoon, based on the WBSEDCL's convenience, workload, and internal planning.

e. All hands-on labs shall be delivered using virtual or simulated environments, along with read-only access to the production controllers, to ensure practical learning without any risk to live services. Where feasible, the WBSEDCL's existing virtual

lab setup in this project may be utilized; however, all training activities shall use separate lab-specific configuration files or isolated topologies that do not interfere with or modify any primary production configuration or network architecture

f. All training material (presentations, manuals, SOPs) must be provided in both hard and soft copy. All costs related to training—including trainer travel and accommodation, printed and digital training materials, and any other associated expenses—shall be borne by the bidder. WBSEDCL will not provide any separate financial support or logistical assistance for training execution.

g. **Training Plan and Content Overview-**

Training Module	Key Topics Covered	Duration (3.5 hrs/day)
SD-WAN Operations	- Controller/Orchestrator GUI usage - Device onboarding, hybrid site configuration - Policy-based routing, SLA profiles, failover testing - Internet breakout rules (user/group based) - Tunnel diagnostics, link health monitoring - Practical labs: policy creation, failover simulation, config backup & restore	2 Days
Managed Switches	- VLAN configuration, port security, storm control - Link aggregation (LACP) - Switch controller GUI usage - Config backup/restore - Lab: VLANs,config backup and restore	1 Day
NAC (Network Access Control)	- Device profiling and posture validation - AD/LDAPS integration - Guest access workflows - MAC authentication and 802.1X testing - Lab: posture test, AD-based login, monitoring NAC events	1 Day
Wi-Fi Controller & Access Points	- Wi-Fi controller GUI overview - SSID creation, VLAN mapping, captive portal/802.1X - AP onboarding, RF/channel/power settings - Roaming optimization (802.11r/k/v) - Client troubleshooting (RSSI/SNR) - Lab: SSID creation, AP onboarding, RF tuning	1 Day
Internet Traffic Control & Logging	- Internet breakout and bandwidth control policies, Captive portal config, dashboard messages, troubleshooting user login and logout issue's, assigning access to users and groups - URL/app filtering - Log searching & device/user correlation - Alert configuration wrt users/bandwidth - Lab: create policies, alerts, log search	1 Day
Reports & Analytics	- Real-time and historical dashboards - WAN SLA reports, uptime, device health - Wi-Fi, NAC, switch & SD-WAN analytics - Custom report creation and scheduling - Lab: monthly SLA report, custom Wi-Fi client report	1 Day
Troubleshooting Workshop	- Tunnel issues, packet loss, latency analysis - Wi-Fi interference and client disconnect issues - NAC authentication failures - Packet capture analysis	0.5 Day

	- Simulated incident response	
Security & SOP Documentation	- Role-based access control, password policies - Certificate management (NAC/Wi-Fi) - Firmware upgrade & rollback procedure - SOP creation for SD-WAN, Wi-Fi, NAC, switches	0.5 Day

34. **Virtual Lab Environment**- The Bidder shall design, supply, configure, and maintain a fully functional Virtual Lab Environment based on EVE-NG Professional/ Corporate Edition or an equivalent enterprise-grade network emulation platform for entire project period. The lab shall replicate real or near-real production workflows and support activities such as configuration validation, integration testing, troubleshooting, and training as mentioned in detail in technical annexure.

    a. The Bidder shall ensure adequate hardware/software sizing so that all virtual images operate seamlessly in a single topology. Any performance, compatibility, or resource issues identified during the project shall be resolved by upgrading hardware or software at no additional cost.

    b. An initial Virtual Lab setup with basic connectivity shall be demonstrated, including at least two SD-WAN edge devices, one SD-WAN Controller, two switches, PC/endpoints, and two WAN links. This baseline topology shall be operational during delivery and installation of Data Centre related materials and detailed configurations shall be progressively updated in the lab as the project configuration evolves and should be completed before final installation of all devices.

35. The Bidder shall conduct comprehensive **Preventive Maintenance (PM)** for the entire SD-WAN and associated network infrastructure as detailed below:

    a. **PM Frequency ,Scheduling and Billing-**
        1) Preventive Maintenance shall be carried out once every six (06) months for all supplied and installed components, and must be performed by the Bidder's designated personnel through physical visits to all offices/sites.
        2) A minimum gap of 120 days must be maintained between two successful PM cycles.
        3) The PM cycle shall commence from the Go-Live date, and a total of ten (10) Preventive Maintenance cycles must be completed during the entire project period. Since each PM is performed every six (6) months, any SLA penalties arising from missed, delayed, or incomplete PM activities will be deducted from the every warranty/maintenance bills (i.e., the bill cycles that coincide with PM completion). The Bidder shall therefore ensure timely submission of all PM hardcopy certificates along with the consolidated summary Excel report for each completed PM cycle.
        4) PM schedules must be mutually agreed with WBSEDCL and performed without impacting live services.

    b. **PM Coverage – Devices, Components and sites**
        1) DC DR devices- Configuration review—aligned with ISO 27001:2022 or the latest applicable standards and WBSEDCL's processes—shall be conducted. This review shall cover

software/firmware versions, routing configurations, tunnel status, controller synchronization, security hardening, and overall device health of all devices in DC DR and all Wi-Fi access points.

2) **SD-WAN Edge Devices and Managed Switches –** Preventive Maintenance and Configuration Review**.** The Bidder shall perform preventive maintenance for all SD-WAN edge devices, managed switches, including physical inspection (cable condition, dust removal, airflow clearance using blowers, etc.) through on-site visits at the respective office locations. In addition, a centralized configuration review—aligned with ISO 27001:2022 or the latest applicable standards and WBSEDCL's processes—shall be conducted. This review shall cover software/firmware versions, routing configurations, tunnel status, controller synchronization, security hardening, and overall device health for all SD-WAN edge devices , managed switches.
3) Verification of NAC agent and TLS Inspection / SSL Decryption Certificates in all end points of the offices.

c. **Documentation & Reporting** –

1) A Preventive Maintenance certificate must be submitted for each site, duly signed by the Site In-charge/authorized representative. The certificate shall clearly mention:
2) PM performed for SD-WAN edge devices, managed switches.
3) Summary of endpoint (PC/laptop) compliance – number of systems with NAC agent and TLS/SSL inspection certificates, and those without, along with recorded reasons for non-compliance.
4) An incident must be raised under the PM category by the designated personnel at HQ/DC upon receiving the scanned copy of the signed PM certificate from the site-visiting PM personnel via the official email ID provided by the bidder. The designated personnel shall then upload the scanned PM certificate to the WBSEDCL's incident reporting system.
5) The date of the incident recorded in the system will be treated as the official PM date and will be used for SLA compliance calculations, including determining the number of days between the current and previous PM cycles.
6) A consolidated preventive maintenance and configuration review report shall be maintained in Excel or CSV format for each site. The report shall include, at minimum: Site Name, IP Address, SD-WAN Device Serial Number, Switch Serial Number, PM Status, Configuration Review Status, Current PM Date, Previous PM Date, Difference in Days, Incident Number, Incident Date (PM Date), Total Number of PCs, Number of PCs Without NAC Agent, Number of PCs Without TLS/SSL Certificate, and a Remarks/Observations Summary.
7) A separate consolidated report shall be maintained for the DC-DR environment, including configuration review remarks and detailed device/server information.

36. Manpower and Resource deployment- During delivery and installation, the Bidder shall deploy adequate resources as required to ensure that project timelines are met while fully adhering to the RFP's IT security requirements and the WBSEDCL's guidelines and policies. The bidder is

required to provide qualified and trained personnel for effective on-site operations, configuration, maintenance, and support of the SD-WAN and associated network infrastructure as per requirement. Compliance with Indian labor laws, cybersecurity policies, and WBSEDCL's policies is mandatory.

37. Minimum Resource Requirements: Deployment, Availability, Service Windows, Qualifications & Certifications (related documents to be submitted for verification after successful LOA placement if bidder qualifies)

Sl No	**Resource**	**Resource Deployment, Availability & Minimum Staffing Requirements**	**Minimum Qualification / Certification / Remarks**
1	L1-Site Visiting Personnel (Installation, Issues & PM Support)	Deployed on-site as needed for installation, basic troubleshooting, physical inspection, and PM activities by bidder.	Technical Knowledge: • Basic understanding of computer hardware, OS/software, LAN cabling, and identification of router/switch/SD-WAN ports and indicators. Other Requirements: • Basic communication skills for interacting with branch/office staff. • Background verification to be done by bidder. • The bidder shall ensure that all deployed L1 resources receive basic operational awareness related to ISO 27001:2022 as applicable to their duties. (An undertaking shall be submitted by the bidder confirming that this above requirement will be maintained for all deployed L1 resources throughout the project period.)
2	L2 Engineer-Onsite Personnel at DC,DR,VB	For maintenance and service: • Data Centre (DC): Minimum one (1) dedicated personnel available 365x24×7. • **Headquarters (VB):** Minimum one (1) personnel during office hours. • **Disaster Recovery (DR) Site:**	• Educational **Qualification:** B.Tech (CSE/IT/ECE), MCA, or Graduate with recognized computer networking certifications such as CCNA or higher. • **OEM Certification:** Certification in the OEM's SD-WAN solution. • **IT Security Knowledge:** Must have basic IT security knowledge, either through formal coursework or any relevant introductory certification.

		Minimum one (1) personnel during office hours, Personnel may be called outside office hours based on special or emergency requirements. • **Additional Resource Requirements**: Additional personnel shall be provided at DC/DR/VB as and when required during upgradation, migration, testing, cutover activities, or any other critical operations, irrespective of time.	(certification/undertaking from bidder) • **Experience:** Minimum 2 **years of experience** in handling Firewall/SD-WAN solutions. (undertaking by bidder) • **Standards Awareness:** Awareness and working knowledge of **ISO 27001:2022**. (undertaking from bidder) Working knowledge of basic network security and troubleshooting tools such as Nmap and Wireshark, basic Python scripting for automation and analysis, and operational exposure to managed switches, VLAN configuration, Wi-Fi and NAC / AAA-based access control.**Other Requirements:** • Background verification of the personnel shall be carried out by the bidder *(an undertaking shall be submitted by the bidder).* • Deployed personnel shall be on the bidder's **direct payroll**.
3	L3 Engineer-Senior technical expert	(Flexible / On-Call), Minimum 1 Nos, But should be made available **onsite within 2 hours** in case of any urgent requirement of the WBSEDCL's, in addition to the existing onsite resident engineers. The L3 engineer shall remain engaged until the issue is resolved or until the WBSEDCL determines otherwise.	• **Educational Qualification:** B.Tech (CSE/IT/ECE), MCA, or Graduate with CCNA/CCNP or higher-level computer networking certification. • **OEM Certification:** Certification in the OEM's SD-WAN solution. • **IT Security Knowledge:** Must possess IT security knowledge supported by at least one globally recognized cybersecurity certification at practitioner level, such as CEH or CompTIA Security+, or any higher-level security certification acceptable to the WBSEDCL. • **Experience:** Minimum 5 **years of experience** in handling Firewall/SD-WAN solutions.

			(undertaking from bidder) • **Standards Awareness:** Awareness and working knowledge of **ISO 27001:2022 (**. undertaking from bidder) **<u>Other Requirements:</u>** • Background verification of the personnel shall be carried out by the bidder *(an undertaking shall be submitted by the bidder).* • Deployed personnel shall be on the bidder's **direct payroll**.
4	Project Manager / SPOC – Non-Technical Management Role & Technical Oversight)	(Flexible / On-Call), Minimum 1 No.	The bidder shall provide an **official letter of assignment/authorization** designating the individual as the Project Manager/SPOC for the project. **<u>Other Requirements:</u>** • Background verification of the personnel shall be carried out by the bidder *(an undertaking shall be submitted by the bidder).* • Deployed personnel shall be on the bidder's **direct payroll**.
5	Network Architect	Flexible/On call and during start of project.(Minimum 1 no)	Network Architect – Minimum Eligibility, • Has a minimum of 5 years of experience in Network Architecture and Enterprise Network Design. • Has prior experience in designing DC/DR network architecture, including redundancy and high availability. • Has hands-on experience in SD-WAN design and implementation in a multi-site enterprise environment. • Has worked on at least one project involving 100+ sites or equivalent large enterprise WAN deployment. Supporting documents to be submitted:

			Bidder-certified experience summary as requested above ,Relevant certifications (if available)

38. Job Roles: L1, L2, L3 Engineers and Project SPOC-

A. L1 – Site Visiting Personnel (Field Support)
   a. Assist with installation, cabling, device placement, and basic setup.
   b. Perform simple troubleshooting (power, cables, LED/port checks).
   c. Support PM activities under L2 guidance (cleaning, physical checks).
   d. Conduct site surveys and assist with NAC agent installation.
   e. Provide field updates, photos, and checklists to L2.

B. L2 – Onsite Engineer to be deployed at DC/DR/VB
   a. Configure, manage, and support SD-WAN devices, controllers, switches, Wi-Fi controllers/APs, NAC,AAA appliances, log servers, Reporting Analytics,Virtual Lab and LAN/WAN infrastructure.
   b. L2 personnel shall perform operational and support tasks as assigned by WBSEDCL, and the allocation or split of duties among deployed resources shall be decided by WBSEDCL based on operational requirements.
   c. L2 personnel shall execute operational activities as per approved designs, configurations, and procedures defined by the WBSEDCL and coordination with L3 team.
   d. Daily reporting of critical alarms and incidents, and periodic (weekly) reporting of non-critical alerts. Monitoring of controller health (SDWAN,Managed switch,NAC/AAA ,Log server dashboards) and failover status between DC and DR and immediate reporting of failover issues.
   e. Maintain Virtual lab and knowledge of it. Execution of patch testing and validation activities in the SD-WAN / switch lab as per approved procedures. Also pushing and deployment of patches for all devices in this project.
   f. Perform routing, switching, VLAN, QoS, and policy configuration, port security for each users (mac binding with port and maintenance) , and guidance to users and monitoring.
   g. DHCP operations for DC/DR/VB as per approved design, including static bindings, hybrid DHCP usage, IP–MAC bindings, and maintenance of DHCP snooping / binding tables as configured.
   h. Operational support for FQDN, DNS resolution, and related services required for ZTP and controller/device onboarding. Also VPN and ZTP related support guidance to users.
   i. Preparation of user manuals for ZTP and other required services related to this project for easy user following.
   j. Implement security controls including URL/IP filtering, access policies, and NGFW/SD-WAN rules. NAC-AAA integration with LDAP,LDAPS,AD and daily updates and maintain role based access for all devices in this project.
   k. Review and apply IOCs from CERT-In / NCIIPC and maintain logs of applied/pending indicators.
   l. Coordinate with SIEM, AD/LDAPS, DNS, NTP, NMS,EDR and WBSEDCL teams for integrations and issue resolution. Operational coordination for middleware-based threat management and log server/SIEM integration
   m. Certificate lifecycle management for all certificates used in the project (SDWAN ,TLS SSL inspection for users etc) , including monitoring validity, renewals, and coordination to prevent service impact. On-site and remote support for

installation and renewal of NFA agents and TLS certificates (for TLS SSL inspection), with scheduled renewals and interim remote guidance.

n. Manage end-to-end user lifecycle across SD-WAN, Switch, and NAC-AAA systems, including onboarding new users, admin users, updating access and authorization based on LDAP, LDAPS or ERP systems, and removing retired or terminated users. Conduct regular access reviews and updates through automated or manual processes on a daily, weekly, or monthly basis in accordance with WBSEDCL's policies.
o. Monitor system alerts and immediately report potential security threats to the WBSEDCL's IT Security Team.
p. Log incidents in the WBSEDCL's incident management tool and update status until closure.
q. Provide RCA inputs for incidents when requested and support the L3 team during detailed RCA preparation.
r. Shall perform authorized basic network discovery and hygiene scans using Nmap or equivalent tools, such as active host discovery, open port and service identification, with monthly/quarterly reporting as decided by WBSEDCL.
s. Maintain device inventory, backups, replacements, movement records, and updated network diagrams.
t. Daily management of user internet access, including captive portal administration, and granting or restricting site access for users or groups as per WBSEDCL's requirements. Implementation and day-to-day management of approved internet access control profiles and policies.
u. Daily monitoring of outbound data traffic over ILL links, including host, application, IP, port, and service visibility, with timely alerts and coordination through integration and compliance with the ILL ISP DDoS mitigation portal, as per WBSEDCL's requirements.
v. Provide **daily/weekly/monthly reports** (as required) on device health, incidents, PM activities, alerts, and utilisation.
w. Assist during internal/external **audits**, compliance checks, and support VAPT teams by providing logs, configurations, snapshots, and evidence as needed.
x. Do necessary troubleshooting of issues and Coordinate effectively with L1, L3, link vendors, SI teams, and escalate issues as per the approved escalation matrix.
y. Provide remote support, management, and guidance for WBSEDCL's office in New Delhi.
z. Visit DC/DR/VB/ALDC/other WBSEDCL sites when required and attend trainings related to IT security awareness as required by WBSEDCL.

C. L3 – Senior Technical Expert (Escalation)

a. Attend meetings as required, including monthly progress and status review meetings.
b. Possess advanced expertise in devices and solutions in this project as SD-WAN, Managed switch, NAC-AAA, Log server, Virtual Lab architecture, network security, troubleshooting and automation, provide remote oversight and guidance to L2 teams and shall be available on an on-call / requirement basis for complex issues, design validation, and major incident resolution.
c. Provide expert troubleshooting for complex SD-WAN, firewall, routing, and security issues.
d. Provide expertise and guide in network architecture designing and upgradation or changes during project period.
e. Documentation submission and updating.
f. Perform RCA, deep diagnostics, and recommend corrective actions.

g. Support design review, configuration optimization, and architecture-level changes.
h. Assist during upgrades, migrations, DR drills, and critical incidents.
i. Coordinate with OEM TAC for L4 escalations.
j. Guide L1/L2 engineers and validate resolutions.
k. Remain on-call and visit onsite for high-priority technical requirements and issues not resolved by L1/L2 personnel.

D. Project Manager / SPOC (Non-Technical & Technical Oversight)

a. Attend meetings as required, including monthly progress and status review meetings.
b. Act as Single Point of Contact (SPOC) between the bidder and WBSEDCL's.
c. Responsible for assignment, oversight, and coordination of onsite personnel.
d. Accountable for proper device delivery at new/shifted sites.
e. Ensure roadmap targets, rollout plans, and timelines are achieved.
f. Submit monthly progress reports and attend scheduled review meetings (weekly during implementation).
g. Ensure smooth rollout and operation of this network upgradation project.
h. Handle issues not resolved by assigned personnel.
i. Manage escalation, coordination, and closure of project-related issues.
j. Payment and billing related matters resolution with accounts team.
k. Maintain communication with WBSEDCL's representatives and ensure timely resolution of all issues.

39. The Bidder shall assign its official email IDs to all personnel deployed under this project and shall ensure full compliance with the WBSEDCL's email usage, security policies and access security policies (Annexure- Access security Policy). All project-related communication shall be carried out exclusively through the Bidder's official email accounts, and the Bidder shall ensure the safety and security of all such email communications.

40. The Bidder's deployed personnel shall be available for emergency duties outside normal office hours, including nights, weekends, and public holidays, as required by the WBSEDCL. The Bidder shall arrange and bear the cost of transportation, lodging, and logistics for such emergency deployments.

41. The Bidder shall ensure continuity of support staff and avoid frequent rotation of L2/L3/SPOC personnel. Any unavoidable replacement shall require a minimum of five (5) days' prior intimation to WBSEDCL, along with advance training and complete knowledge transfer to the incoming personnel. If the Bidder provides less than the required 5-day notice, SLA penalties shall be applied for the shortfall period on a pro-rated basis. For example, if only three (3) days' notice is given, SLA penalties equivalent to two (2) days of personnel non-availability shall be imposed, in accordance with the applicable SLA clause.

42. All deployed L1 personnel shall be officially authorized by the Bidder. The Bidder shall issue valid company ID cards and/or authorization letters, and ensure compliance with all applicable Indian labour regulations. Background verification and adherence to the WBSEDCL's security protocols are mandatory. Prior to any site visit, the Bidder shall send an email notification with the personnel details to the designated official email IDs of WBSEDCL officials. The L2 onsite personnel shall coordinate these communications and ensure proper verification and alignment with the WBSEDCL's procedures.

43. The Bidder shall conduct complete background verification and reference checks for all personnel deployed under this project and shall submit an undertaking confirming the completion of such verification for each deployed resource.

44. The Bidder shall submit full details of all L2, L3, and SPOC personnel, clearly mentioning their name, employee ID, ID card number, background verification status, and all other relevant identification and verification particulars. In the event of any personnel change, the Bidder shall promptly update and resubmit the undertaking and complete personnel details without delay.

45. The Bidder shall provide all personnel in this project with the required training, refreshers, and upskilling sessions throughout the project period to ensure they remain fully updated and competent in operating, managing, and supporting the deployed solution.

46. Access to the WBSEDCL's Data Centre (DC), Disaster Recovery (DR) site, and any other designated critical locations shall be strictly controlled. The Bidder's personnel may visit such sites only after obtaining prior written permission from the WBSEDCL and submitting all required documentation (including ID proof, authorization letters, and visit requests) in advance. Entry shall be permitted solely upon formal approval and completion of the WBSEDCL's due-process requirements for physical access, visitor registration, and device sanitization.

47. All laptops, tools, storage media, and any other devices carried or used by the Bidder's personnel during installation, maintenance, or support activities shall be malware-free, fully compliant with industry-standard cybersecurity practices, and subject to security inspection at the entry and exit points. The Bidder shall ensure that no unauthorized removable media, network adapters, or monitoring tools are brought into DC/DR or critical areas without explicit approval from the WBSEDCL.

48. The Bidder shall also ensure full adherence to the WBSEDCL's access protocols, security guidelines, asset handling procedures, and device sanitization policies applicable to restricted environments.

49. The Bidder shall ensure that all deployed personnel strictly adhere to the WBSEDCL's discipline, office decorum, and professional conduct standards while on premises or performing project duties. The Bidder shall remain fully responsible for the proper execution of all assigned roles, scope of work, deployment requirements, and performance obligations. Any lapse in conduct, behavior, deployment, or performance by the deployed personnel shall be the sole responsibility of the Bidder.

50. The Bidder shall follow all onboarding and de-onboarding procedures as per ISO 27001:2022 /latest requirements and the WBSEDCL's latest security policies, including the issuance and revocation of access rights, ID cards, email accounts, and system permissions. The Bidder shall ensure immediate and complete deactivation of all access privileges for any personnel exiting the project. All deployed personnel shall strictly adhere to the confidentiality obligations and NDA provisions specified in the NDA Annexure. Any breach of confidentiality, misuse of access, or violation of security requirements by the Bidder's personnel shall be the sole responsibility of the Bidder.

51. The Bidder shall provide all required tools, safety equipment, testing devices, cleaning materials, and consumables necessary for installation, preventive maintenance, and site visits. The Bidder shall ensure that all personnel are adequately trained and equipped to work safely

in compliance with government standards. A preventive maintenance format, covering all activities as defined in the Scope of Work, shall be issued by WBSEDCL at the time of placement of the Letter of Award (LoA). Compliance with and execution of preventive maintenance as per this format shall be mandatory for the successful bidder.

52. All personnel deployed under this project shall follow the attendance system prescribed by the WBSEDCL. The attendance records captured through the WBSEDCL's chosen system shall be treated as the official record and shall form the basis for calculating SLA compliance, particularly for L2 onsite personnel availability.

53. The Bidder shall submit a detailed Escalation Matrix covering delivery, installation, POC activities, configuration, migration, and ongoing maintenance for all components under this project. The matrix shall clearly specify the designated personnel at each escalation level—L1 Field Support, L2 On-site Engineers (DC/DR/VB), L3 Senior Technical Expert, Project Manager/SPOC, and respective OEM support contacts—with their names, designations, official email IDs, and contact numbers. Separate escalation paths shall be provided for (a) Delivery & Installation and (b) Technical Support & Operations.

54. The Bidder shall also provide a dedicated support contact number to be published in the WBSEDCL's Helpdesk system. This number shall be answered by the deployed L2 personnel, who will coordinate with other L2, L1, L3, OEM TAC, and all relevant stakeholders as per the approved escalation process. The support number must remain unchanged throughout the entire project duration and shall be submitted before commencement of device installation.

55. The Bidder shall maintain an adequate stock of spare SD-WAN devices, managed switches, SFP modules, power adapters, Wi-Fi Access Points, rack accessories, and all other components supplied under this project. These spares shall be stored and readily available within the State of West Bengal to ensure immediate replacement whenever required. The Bidder shall also maintain a complete and structured hardware replacement process, ensuring that any faulty component—whether SD-WAN device, controller, managed switch, NAC-AAA appliance, Wi-Fi component, Log Server, Reporting/Analytics system, or any associated accessory—is replaced on priority without impacting network operations. Replacement units shall be of the same model, or a higher model/OEM-certified equivalent, and must include the same warranty, support coverage, and software/firmware entitlement as the original device.

56. A detailed assert register document as mentioned in documentation annexure shall be submitted to the WBSEDCL on the Go-Live date, containing the complete and final device inventory. This report shall include, for every site at least. After Go-Live, the Bidder shall submit quarterly device-replacement reports, capturing all devices replaced during the quarter, along with updated information including Location, IP Address, old/new MAC addresses, old/new serial numbers, and warranty status. This reporting shall accompany each half yearly maintenance bill.

57. **Backup and Recovery**-The Bidder shall design, implement, and maintain a comprehensive Backup, Recovery, and Disaster Recovery (DR) Readiness Framework for all components deployed under this project, including SD-WAN Controllers, SD-WAN Edge Devices, Switch Controllers, Managed Switches, NAC–AAA systems, Wi-Fi Controllers, Log Servers, Reporting & Analytics systems, and Virtual Lab components. This framework shall ensure secure backup retention, rapid recovery, full DC–DR resilience, and uninterrupted service availability.
    a. Configuration & Database Backups
        - Daily backups or as per WBSEDCL's requirement of all critical SD-WAN devices, switches, controllers, NAC–AAA, Wi-Fi components, Log Server,

Reporting & Analytics systems at DC, DR, HQ, ALDC locations with high end boxes.
- Site office boxes and switches, monthly or as per WBSEDCL's requirement.
- Backups shall include templates, policies, certificates, system parameters, and database records.

b. Backup Retention & Versioning
- Minimum 90 days retention for device-level backups.
- Minimum 180 days retention for controller/system database backups.
- Maintain minimum 3 historical versions for DC/DR/VB/ALDC and critical location devices and minimum 2 historical versions for site office devices.

c. Backup Infrastructure
- The Bidder shall provision all required hardware, storage (preferably SAN based flash), software, tools, backup repositories, scripts, encryption utilities, and other components required for performing, storing, and managing backups at DC and DR without any additional cost to the WBSEDCL. And backups should be stored as per WBSEDCL's requirements.

d. Security & Encryption
- All backups shall be stored in encrypted form (AES-256 or higher).
- Backup repositories must enforce RBAC, strong access control, and mandatory audit logging.
- Backup processes shall fully comply with ISO 27001:2022, or latest, NCIIPC, CERT-In guidelines, and WBSEDCL security policies.

e. Recovery
- Restoration of any SD-WAN device or switch must be possible within 4 hours or as per WBSEDCL requirement.
- Restoration of controllers (SD-WAN, Switch, Wi-Fi), NAC/AAA, Log Server, reporting Server within 4 hours or as per WBSEDCL requirement.
- Must support full operational recovery without configuration drift.

f. Quarterly Backup Reports
- Backup & Recovery Report shall be submitted as per WBSEDCL requirement.
- The report shall include info regarding backups taken, frequency, status of backups restorations etc.

58. DR Drill -
    a. The Bidder shall conduct a full DR Drill at least once every year and additionally as per WBSEDCL's DR/BCP policy for devices/solutions in scope of this project
    b. The drill shall validate SD-WAN controller failover, Switch controller failover, NAC/AAA failover, Log Server and Reporting Server cutover, tunnel regeneration, policy/template synchronization, and user authentication flows.
    c. For each drill, the Bidder shall submit detailed documentation as per ISO 27001:2022 or latest compliance, including the execution plan, steps performed, observations, failover performance metrics, issues identified, and corrective/preventive actions.

59. All storage systems used or supplied under this project shall be enterprise-grade and based on modern storage technology, supporting industry-standard RAID configurations (RAID-5/10 or higher) to ensure data redundancy, performance, and fault tolerance. The storage must provide secure access controls, encryption support, hot-swap capability, and sustained I/O performance suitable for 24×7 operations. It shall efficiently handle all required data volumes—including logs, backups, analytics, configurations, reports, and system events—and must remain fully

scalable to meet current and future storage demands throughout the project duration, in compliance with OEM best practices and WBSEDCL's security standards.

60. If any subdomain is required for deploying project components, WBSEDCL will provide the necessary domain names and DNS/subdomain mappings as per its approved naming convention. However, the Bidder shall be solely responsible for procuring and deploying all required SSL/TLS certificates for secure communication. This includes certificates needed for any application, device, management interface, API, controller, ZTA-related security requirement, or any other component delivered under this project. All such certificates must be valid, CA-signed, and supported throughout the project duration.

61. Upon completion of the project period, the Bidder shall hand over to WBSEDCL all licenses, hardware, software, firmware, configuration files, documentation, access credentials, and any other project-related deliverables in fully functional and transferable condition. The Bidder shall ensure that all licenses are valid, active, and legally transferable, and that no component of the solution remains under the Bidder's ownership, control, or restriction after handover.

62. All project-related materials—including licenses, hardware, software, firmware, documentation, configurations, and deliverables—shall remain in the name of WBSEDCL from the outset of the project. Upon completion/termination of the project, the Bidder shall hand over to WBSEDCL all such assets in fully functional and transferable condition, including all access credentials, configuration files, and supporting documents. All licenses shall remain valid, active, and legally transferable to WBSEDCL, with no ownership, control, or operational dependency retained by the Bidder. The Bidder shall also strictly adhere to the Non-Disclosure Agreement (NDA) requirements as specified in the NDA Annexure throughout the project and during the handover process.

63. Proof of Concept (POC) and Acceptance testing-The POC shall function as the initial Acceptance Testing stage, specifically validating the bidder's capability to implement the SD-WAN and Switching solution proposed in this project. The POC must demonstrate that the bidder can successfully deploy, configure, integrate, and operate the SD-WAN and Switching components as per the Technical Specifications, Security Requirements, and Solution Architecture defined in this RFP.
    a. The Bidder shall initiate the POC by deploying a qualified team to survey the designated locations and assess the existing infrastructure. Based on this assessment, the team shall prepare the POC network design, covering connectivity between the two POC locations and the Controller (whether hosted on-site or on the cloud).
    b. The Bidder shall demonstrate the physical deployment at a minimum of two WBSEDCL selected sites (in and around Kolkata or Berhampore). The requirements for the physical POC are as follows:
    c. SD-WAN & Switch Hardware- Each POC site shall include one SD-WAN appliance and one managed switch of the same make and model proposed for actual deployment at site offices, as specified in the SD-WAN Technical Annexure.
    d. Laptop/PC for Testing-The Bidder shall provide at least one laptop/PC at each POC site for end-to-end testing and validation activities.
    e. Controller Hosting (On-Prem or Cloud)-The SD-WAN and Switch controllers for the POC may be hosted either on-premises or on the cloud, at the Bidder's convenience. All required functionalities of both controllers must be demonstrated in full, irrespective of hosting mode.

f. Internet Links-The WBSEDCL shall provide Internet links at each POC site, as per its choice and availability.

g. Accessories & Installation Materials-All other required items—including cables, power adapters, tools, devices, installation materials, and accessories—shall be provided entirely by the Bidder.

h. Security-At no stage shall WBSEDCL's' traffic or production network be merged with, impacted by, or routed through the POC setup. The Bidder shall ensure complete isolation between the POC environment and the WBSEDCL's live network, and shall implement all necessary safeguards and precautions to prevent any form of interference or leakage between the two.

i. Technical Demonstration Requirements:

I. Routing functionality (static/dynamic as applicable).
II. Overlay & Underlay tunnel formation and tunnel health.
III. Device reachability, controller–device synchronization and registration workflow.
IV. Template deployment, provisioning workflows, and configuration push validation.
V. Policy enforcement (application policies, path selection, traffic steering, firewall/policy rules where applicable).
VI. WAN dual-link performance including failover, SLA-class behavior, jitter/loss response.
VII. Switch functionalities including VLANs, L2 behavior, trunk/access ports, uplink redundancy etc
VIII. Performance monitoring, dashboards, alerts, logs, and device statistics as in Controllers.
IX. Compliance with SD-WAN and Switching Technical Annexure for POC set up applicable features.

64. The Bidder shall prove configuration accuracy, solution stability, and deployment readiness through these demonstrations. WBSEDCL's evaluation and acceptance of POC performance shall be final and binding.

65. POC Outcome & Consequences- The Bidder shall successfully complete all activities of the POC as specified above. **No payment shall be made** for any work carried out during the POC/Acceptance testing. Based on the WBSEDCL's evaluation—whose decision shall be final and binding—the following outcomes shall apply**:**

a. **If the POC is successful:**
   1) Submission of the complete successful POC report, including all required snapshots, POC topology diagrams, logs, screenshots, configuration backups, and any other supporting documentation demonstrating the successful execution of the POC.
   2) Upon placement of LOA -The Bidder shall proceed with all remaining project activities strictly in accordance with the RFP, approved Scope of Work, project timelines /milestones. The bidder shall submit the Detailed Technical Specifications sheet of the product from OEM for all proposed devices and solutions (SDWAN controller, boxes, Switch Controller boxes, NAC -AAA,Log Server,Report Analytics,Network Racks etc) covering hardware specifications, software features, licenses, throughput parameters, performance benchmarks, environmental ratings, and OEM lifecycle information including End-of-Support (EOS) and End-of-Life (EOL). These

documents must be duly stamped and signed by the respective OEM(s) and bidder and shall be reviewed and approved by WBSEDCL.

3) Upon placement of LOA -**The Bidder shall engage a network architect** and prepare and submit a high-level design and detailed Low-Level Design (LLD) for the approved architecture. The LLD shall include configuration-level details such as SD-WAN templates, routing parameters, SLA profiles, switch port/VLAN mapping, NAC posture and authentication flows, captive portal mapping, IP addressing plan, security policies, controller configuration schemas, and site-wise implementation sheets. The project shall transition to subsequent milestones as defined in the Terms of Payment and implementation schedule.
4) Upon placement of LOA-The Bidder shall design and create a network architecture, previous and after upgradation architecture diagrams. Demonstrate the SD-WAN and Switching architecture within the Virtual Lab environment, including SD-WAN controllers, virtual SD-WAN edge devices, managed switches, WAN links/ WAN emulation routers.

b. **If the POC is unsuccessful:**

1) WBSEDCL shall intimate the bidder regarding the unsuccessful POC, and the bidder shall be removed from further consideration for the project. No order shall be issued to the bidder.
2) **Invitation letter to L2 (on POC failure):** In the event of such termination, the L2 bidder may be offered the project, provided they **agree to match the L1 bidder's rate and accept all terms and conditions of the tender.**
3) If the L2 bidder declines or fails to execute the work, the WBSEDCL may approach the **L3 bidder or the next eligible bidder** under the same terms and conditions.

66. The Bidder shall provide all necessary accessories—such as power cords, Ethernet/Fibre patch cables, rack-mount installation accessories (mounting kits, brackets, screws), and any other connectivity components required between SD-WAN devices, switches, or associated equipment—at their own cost during SD-WAN device installations at all locations. All cables shall be properly organized, dressed, and tied using suitable cable-management materials to ensure a neat, safe, and compliant installation.

67. All manuals, documents, and device specifications related to this project shall be provided in English. The Bidder shall supply complete specification sheets and technical documentation for all devices included under this project.

68. All devices, hardware, firmware, and software provided by the Bidder must be fully supported by their respective OEMs for the entire duration of the project. No component supplied under this project shall be at, or nearing, End-of-Support (EOS) or End-of-Life (EOL). The Bidder shall ensure and certify that all proposed devices and software will remain under OEM support, updates, and services throughout the complete project period.

69. The Bidder shall submit complete product and asset information for all devices supplied or deployed under this project, including brand, model number, serial number, printed product brochures, and technical specification sheets. The respective OEMs/vendors shall provide End-of-Support (EOS) and End-of-Life (EOL) details for all hardware, as well as license validity and lifecycle details for all software used in this project.

70. The Bidder shall maintain and submit detailed asset information for every device supplied or deployed under this project, in alignment with ISO 27001:2022 or latest asset-management requirements. The asset register shall be maintained in Excel format and updated progressively as the project advances. Initial asset details shall be submitted along with delivery milestones and subsequently updated whenever new devices are installed, moved, or commissioned.

71. The asset register may include (but is not limited to) the following preferred fields: Asset Type, Brand, Model No., Serial No., Device Role, Location (if available), IP Address (when assigned), MAC Address (if applicable), Firmware/Software Version, License Type, License Validity, EOS Date, EOL Date, Date of Installation, Owner/Custodian, Remarks.

72. The L2 onsite personnel deployed by the Bidder shall be responsible for maintaining and updating the asset register for all devices under this project, in coordination with the WBSEDCL's team

73. The Bidder shall supply and configure all devices, components, and solutions required under this project and ensure that they are fully operational with the desired performance levels within the stipulated project timelines. Time, quality, and the specified quantity shall be considered the essence of this order. Failure to adhere to the approved timelines, quality standards, or quantity requirements shall entitle the WBSEDCL to rescind the work order without any claim for compensation or damages by the vendor/supplier/agency. Upon such rescission, the WBSEDCL shall be entitled to take punitive action as per the provisions of the tender and work order conditions.

74. The Bidder is expected to be fully acquainted with all local conditions and factors that may affect the performance of the contract and/or the overall project cost. All devices, equipment, and solutions supplied under this project shall operate seamlessly on a 24×7×365 basis under all weather, climatic, and temperature conditions prevalent across all locations of the WBSEDCL.

75. All devices, equipment, and solutions offered under this project shall fully comply with the rating, functional, performance, and feature requirements specified in their respective Technical Annexures and Data Requirement sections. The Bidder shall ensure that every supplied component— including SD-WAN edge devices and controllers, managed switches and switch controllers, NAC–AAA systems, Wi-Fi controllers and access points, Log Servers, Reporting & Analytics platforms, and all supporting modules—meets the mandated technical specifications and delivers the required throughput and performance under full feature load (including routing, security, DPI, TLS inspection, policy enforcement, and monitoring). All devices must operate at or above the defined performance benchmarks throughout the project duration.

76. Wherever REST APIs or programmatic interfaces are used under this project (including SD-WAN, Switch Controllers, NAC/AAA, Log Server, Reporting, Wi-Fi Controllers, and related integrations), they shall be implemented and consumed in accordance with industry-standard security practices. All APIs must enforce secure authentication and authorization (such as OAuth 2.0 or token-based mechanisms), encrypted communication over TLS 1.2 or higher, role-based access control (RBAC), and comprehensive audit logging. API endpoints shall be hardened against unauthorized access, misuse, and common vulnerabilities, and all critical API logs shall be forwarded to the centralized Log Server/SIEM.

77. Wherever web-based management interfaces, dashboards, portals, or administrative consoles are used under this project, they shall be secured in accordance with industry-standard web

security practices. All web interfaces must enforce HTTPS using TLS 1.2 or higher, strong authentication (including MFA where applicable), role-based access control (RBAC), secure session management, account lockout mechanisms, password policy enforcement, and protection against common web vulnerabilities (including OWASP Top 10 risks).All administrative activities and login events shall be logged and forwarded to the centralized Log Server/SIEM for monitoring and audit compliance.

78. The Bidder shall ensure that all devices, components, and equipment supplied under this project comply with the environmental, electrical, safety, and physical installation requirements specified in the technical annexures and OEM guidelines. All supplied equipment must operate reliably within the WBSEDCL's site conditions and must remain fully functional under 24×7×365 operation.

79. All proposed devices and solutions in this project—including SD-WAN devices, controllers, switches, Wi-Fi components, NAC, AAA, logging, reporting systems, Virtual lab,and all other network infrastructure—must fully comply with the General Compliance Requirements defined in the relevant Technical Annexure for each respective component. These requirements cover essential aspects such as standards adherence, security controls, OEM obligations, logging, monitoring, high availability, and overall governance. The bidder shall ensure that every device and solution offered meets these general compliances in addition to the detailed technical specifications provided for each respective device/category.

80. SDWAN -The SD-WAN devices proposed under this project shall maintain full support for all underlay transports (MPLS, ILL, broadband) and establish secure, encrypted overlay tunnels in active-active mode with intelligent load-balancing and automatic failover.

    a. The Bidder shall supply, license, install, configure, integrate, commission, operate, and support SD-WAN devices of the following categories and quantities:

        1) Type-A1 SD-WAN devices (approximately 692 numbers) for small and medium locations supporting around 30–50 users/devices per site;

        2) Type-A2 SD-WAN devices (approximately 50 numbers) for larger locations supporting approximately 200–300 users/devices per site;

        3) High-end SD-WAN devices comprising Type-B1 (4 numbers) for DC DR , Type-B2 (2 numbers), and Type-B3 (2 numbers) for HQ locations, as per the Technical Specifications.

    b. Each device must deliver complete enterprise-grade routing (static, OSPF, BGP), application-aware traffic steering, QoS, DPI, and SLA-based path selection to ensure stable and optimized WAN performance. Integrated security functions including NGFW, IPS/IDS, URL filtering, anti-malware, TLS/SSL inspection, and identity-based policy enforcement must operate without degrading throughput, which must meet the minimum capacities defined for each device type.

    c. The SD-WAN box must also support DHCP Server services, NAT/NAT-T, VRF-based segmentation, L2/L3 features, DNS forwarding, threat-intelligence integration, and seamless interoperability with switches, Wi-Fi, NAC/AAA, and DC/DR services.

d. All routing, traffic management, performance features, security functions, lifecycle controls, and hardware requirements shall fully comply with the detailed technical specifications defined in the Technical Annexure related to SD-WAN devices.

e. All SD-WAN devices must support MPLS, Broadband, Internet Leased Line (ILL), and Point-to-Point (P2P) connectivity, with the ability to use these links simultaneously or selectively as per WBSEDCL's requirements.

81. The selected Bidder shall supply, configure, and support two hundred (200) ZTNA VPN user licenses, inclusive of all required software features, updates, upgrades, and OEM support, for secure remote access to WBSEDCL applications and resources. The Bidder shall be responsible for end-to-end deployment, integration with the existing SD-WAN, NAC/AAA, directory services, and security infrastructure, and for ensuring uninterrupted operation throughout the contract period.

82. In addition, the Bidder shall operate and maintain a centralized **Jump Server**, which shall be configurable, as per WBSEDCL's requirements, in either browser-based access mode or client/application-based access mode. The hardware and base operating system licenses for the Jump Server shall be provided by WBSEDCL, whereas the Bidder shall be responsible for day-to-day operations, continuous monitoring, security hardening, user access configuration, performance management, backup coordination, log monitoring, patch management, vulnerability remediation, and preventive and corrective maintenance of the Jump Server environment.

83. The Bidder shall ensure that the Jump Server and ZTNA VPN services are maintained in a secure, compliant, and highly available manner, with documented procedures, audit logs, and adherence to applicable security policies and SLAs. Daily reporting for VPN access to be provided as per WBSEDCL's requirement.

84. Centralized SDWAN Controller -The SD-WAN Controller/Manager/Orchestrator shall be deployed fully on-premises as a virtual/software appliance with adequate compute resources and must be licensed to manage all Hub and Branch devices at scale, supporting up to 1000 SD-WAN nodes.

a. It shall operate in DC–DR high-availability mode with seamless failover, enabling centralized zero-touch provisioning, template-based configuration, global security and routing policies, live link-performance dashboards, geo-map visualization, and full historical monitoring.

b. The controller must centrally manage all NGFW policies, application signatures, IPS/URL/Geo-IP updates, threat-intelligence (IOC) ingestion, and certificate-based authentication for all SD-WAN devices. It shall integrate with NAC/AAA, AD,LDAP,LDAPS, NMS, SIEM, and other platforms via REST APIs, and provide revision tracking, automatic backups, configuration baselines, audit logs, and rollback capability.

c. The solution must offer multi-user RBAC access, modern secure Web UI, CLI support, NAT-T compatibility, and centralized management of DHCP scopes, DNS policies, and TLS/SSL inspection rules across all sites.

d. All features, controls, and operational capabilities of the SD-WAN Controller shall fully comply with the detailed technical requirements defined in the corresponding Technical Annexure for the SD-WAN Controller.

85. 24-Port Managed L2 Switches- The 24-Port Managed L2 Switches shall provide full Gigabit access connectivity with uplink expansion options and support all essential Layer-2 switching capabilities, including VLANs, trunking, NAC-driven dynamic authorization, 802.1X/MAB, RADIUS VLAN assignment, Change of Authorization, and per-session ACL enforcement.

    a. The switches must offer robust security features such as DHCP Snooping, IP Source Guard, Dynamic ARP Inspection, Storm Control, Port Security, and must interoperate seamlessly with SD-WAN, NAC/AAA, and other network components. QoS, multicast support (IGMP/MLD), port mirroring, loop protection, STP/RSTP/MSTP, IPv4/IPv6 management, SNMPv3, Syslog, SSH/HTTPS, and SIEM integration must be available to ensure stable operations and monitoring.

    b. The switches shall provide non-blocking performance, configuration backups, detailed audit logs, and centralized management via dedicated management VLAN/IP, including cascaded deployment scenarios.

    c. All hardware, performance, security controls, and operational functions shall comply with the detailed technical specifications defined in the Technical Annexure related to Managed L2 Switches.

86. Centralized Switch Controller -The Centralized Switch Controller shall manage the entire switching infrastructure at scale, with capability to centrally monitor, configure, and operate at least 1000 managed L2 switches across all locations.
    a. It must run in a DC–DR high-availability setup with automated backup, synchronization, and seamless failover, while offering a unified dashboard for switch discovery, topology visualization, port status, asset inventory, and traffic analytics.
    b. The controller shall support template-based configuration management with version control, rollback, bulk updates, and role-based approval workflows, enabling consistent onboarding and rapid replacement of switches. Strong role-based access control with centralized AAA server integration and 2-factor authentication must be supported for secure administration.
    c. The system must generate alerts for switch security events such as DHCP snooping violations, MAC flaps, and port-security triggers, and forward all logs and audit trails to the SIEM/log server. It must securely adopt and manage site switches—including cascaded switches—over routed IP/SD-WAN paths, and support automated scheduled backups of all configurations and policies. Open APIs must be available for integration with monitoring, automation, and ITSM tools, along with full switch health monitoring for CPU, memory, temperature, ports, and interface statistics.
    d. All operational, security, and management capabilities shall comply with the detailed technical requirements defined in the Technical Annexure related to the Switch Controller.

87. NAC and AAA- The NAC and AAA solution shall operate fully on-premises with DC–DR high availability and seamless integration with SD-WAN, managed switches, Wi-Fi, and enterprise directory services.
    a. The NAC platform must enforce posture-based access control, dynamic VLAN assignment, quarantine or restricted access for non-compliant endpoints, agent-based and agentless profiling, and scalable handling of all enterprise endpoints with full alerting, dashboards, and compliance reporting.

b. As part of the deployment, the bidder shall be responsible for installing and configuring the NAC agent on all required endpoints by visiting the respective site offices, ensuring complete coverage and proper operational readiness.
c. The AAA system shall provide centralized authentication, authorization, and accounting using RADIUS, TACACS+, integrate with LDAP,LDAPS,AD support role-based policy mapping, log all user sessions, and enforce CoA for dynamic policy changes while scaling to meet all project device and user loads.
d. All required features and controls shall fully comply with the technical requirements defined in the relevant Technical Annexure.

88. Captive Portal - The Captive Portal shall function as the unified authentication layer for both wired and wireless users, enforcing identity verification through LDAP/LDAPS/AD in coordination with NAC/AAA before granting network or internet access.
    a. It must maintain stable session persistence, enforce posture checks, support customizable branding, and provide structured workflows for guest/BYOD onboarding with sponsor approval and time-bound access.
    b. AUP enforcement, device–user association tracking, and large-scale concurrent user support must be available without impacting performance.
    c. All capabilities shall comply with the detailed technical specifications defined in the relevant Technical Annexure.

89. The Internet Traffic Control requirement shall enforce identity-integrated, policy-based governance of all outbound internet traffic, ensuring that only authenticated and posture-compliant users receive access.

    a. This requirement may be fulfilled through a combination of components deployed under this project—such as SD-WAN devices, NAC, AAA, Captive Portal managed switches, Wi-Fi APs, controllers, and log/reporting systems—or through a dedicated on-premises device if required to meet the full functionality.

    b. The architecture must support per-user and per-group identity mapping via directory/NAC integration, granular URL categorization and filtering, application-level visibility and control, and configurable time- and quota-based usage restrictions.

    c. Administrators must be able to apply differentiated allow/block lists at branch, user, and group levels, with seamless integration into SD-WAN for local breakout and routing decisions. Real-time analytics, alerting, and detailed usage reporting by user, device, site, or category shall be supported.

    d. All enforcement behaviors and reporting capabilities shall fully comply with the detailed technical requirements defined in the Technical Annexure related to Internet Traffic Control.

90. Reporting, Dashboard, Analytics -The Reporting, Dashboards and Analytics platform shall provide centralized, real-time and historical visibility for all components deployed under this project, including SD-WAN, managed switches, NAC, AAA and IP address management systems.
    a. The solution must support role-based dashboards for both centralized and regional users, offering customizable views, drill-down analytics, and interactive charts covering link performance, SLA parameters, application and bandwidth usage, device health, security events, and configuration changes.

b. It shall consolidate logs and statistics across all devices, generate scheduled or on-demand reports in standard exportable formats, and retain historical data as required for compliance and audit purposes.
c. The reporting platform must support advanced analytics such as top-talkers, application usage trends, tunnel and link health status, latency/jitter/loss monitoring, downtime reporting, DHCP/IP usage analytics, NAC/AAA posture and authentication trends, switch security events, and certificate/TLS visibility. Integrated alerting through email and dashboard notifications must be available for link issues, performance thresholds, security detections and device-related incidents.
d. The system shall support API-based integration with SIEM, NMS and other enterprise tools.
e. All reporting, dashboarding, analytics and export capabilities shall fully comply with the detailed technical requirements defined in the Technical Annexure related to Reporting and Analytics.

91. SLA-based reporting- The reporting and analytics system shall provide comprehensive SLA-based reporting for all LAN and WAN links as well as SD-WAN and Switch devices, with mandatory retention of all SLA-related data for **a minimum of 2 years**. The system must generate detailed downtime reports—site-wise, month-wise, and vendor-wise—capturing link availability and device-related outages. It shall also record and report latency, packet loss, and jitter incidents across all links, with the ability to detect and log sustained degradation based on WBSEDCL -defined or industry-standard thresholds (e.g., continuous events such as latency, packet loss, or jitter persisting for a set duration). These thresholds may be updated as per WBSEDCL requirements, but the system must consistently track, store, and report these metrics in minutes on a monthly, site-wise, and vendor-wise basis. Additionally, the platform shall provide device failure reports for SD-WAN appliances, Managed Switches and all devices in this project, ensuring full visibility into infrastructure stability. All SLA computation, reporting logic, thresholds, and retention requirements shall be implemented and enforced within the SD-WAN reporting and analytics system.

92. Log Server Solution -The Log Server solution shall provide centralized, secure, and compliant log collection for all components deployed under this project, including SD-WAN devices and controllers, managed switches, switch controllers, Wi-Fi APs, Wi-Fi controllers, NAC, AAA, captive portal, VPN gateways, and Internet access control elements.

a. It **must retain logs in structured, tamper-evident form for a minimum of 180 days** as per CERT-In and ISO/IEC 27001:2022 requirements, and maintain extended SLA-related logs—such as WAN/LAN downtime, SD-WAN device availability, switch availability, and controller availability—for at least two years.

b. The Log Server shall support Active–Active/Active–Passive deployment across DC and DR, dual-ingestion to multiple destinations, and reliable forwarding to SIEM platforms over Syslog (UDP/TCP/TLS) and REST APIs, with rate limiting, batching, retry mechanisms, and complete data fidelity. The system must provide secure archival export, customizable parsing and tagging, alerting for delivery failures, and cryptographic protections (AES-256, TLS 1.2/1.3, signatures, hashing) to ensure confidentiality and integrity of all logs.

c. It shall support centralized, role-based administrative access via the project's AAA platform and be provisioned on adequately sized hardware to accommodate both primary ingestion and future load growth after SIEM integration. The Log Server

must generate audit-ready reports without modifying original logs, maintain NTP-synchronized timestamps, and fully capture the required log types across all SD-WAN, switching, Wi-Fi, NAC, AAA, and supporting components.

d. All features, retention functions, performance expectations, and security controls shall comply with the detailed technical requirements defined in the Technical Annexure related to the Log Server Solution.

93. Virtual Lab- The Virtual Lab Environment shall be delivered as a complete, on-premises emulation platform based on EVE-NG Professional/Corporate Edition or an equivalent enterprise-grade emulator, fully equipped with all required OEM virtual images, licenses, compute resources, storage, and hypervisor infrastructure.

a. The lab must host a production-equivalent topology containing SD-WAN controllers, multiple SD-WAN edge devices, WAN emulation routers, virtual L2/L3 switches, endpoint nodes, DNS/DHCP servers, certificate authority servers, and other supported components, enabling real or near-real configuration, testing, training, and integration workflows.

b. A separate training/development configuration must operate in parallel without impacting the production-equivalent topology. The bidder shall size, supply, and maintain the entire lab environment, ensuring stable performance without degradation; any capacity or compatibility issues must be rectified through upgrades at no additional cost.

c. The lab must remain isolated from production while accurately replicating operational behavior, supporting configuration validation, troubleshooting, role-based access, backup/restore, snapshots, documentation, and topology diagrams. All SD-WAN, switching, or other configuration changes shall be first implemented and validated in the Virtual Lab before deployment to production systems.

d. All features, components, resources, and operational capabilities shall fully comply with the detailed technical requirements defined in the Technical Annexure related to the Virtual Lab Environment.

94. Documentation- The bidder shall provide a comprehensive, ISO/IEC 27001:2022 and latest compliant documentation package covering the complete network design, configurations, operational procedures, and administrative controls for all components deployed under this project.

a. All documents must be submitted in both editable and signed PDF formats and shall be verified and approved prior to Go-Live. Documentation shall include pre- and post-deployment architecture diagrams for DC, DR, HQ, ALDC, and a representative site; a complete IP addressing and allocation plan; high-availability and failover operation details; full configuration records for all SD-WAN devices, switches, Wi-Fi components, controllers, NAC/AAA systems, servers, and other project elements, asset register details.

b. The bidder must also provide detailed workflow documents covering internet access flow, NAC posture, authentication integration, routing and SD-WAN policy behavior, and virtual lab usage. Comprehensive SOPs must be supplied for monitoring, backups, restoration, troubleshooting, escalation, and alarm handling

across all deployed systems. Additionally, a complete administrative access and role management document must list all users with configuration privileges, their authentication methods, privilege levels, and the approved procedures for user lifecycle operations.

c. OEM datasheets for every device must be included, along with a consolidated, version-controlled Master Documentation Package.

d. The bidder shall refresh and update all documentation annually and after any significant configuration, device, architectural, or security changes, without any additional cost.

e. All documentation deliverables and update obligations shall fully comply with the detailed technical requirements defined in the Technical Annexure related to Mandatory Documentation and Go-Live.

95. Wi-Fi Solution-The Wi-Fi solution shall comprise enterprise-grade indoor Access Points and an on-premises Wireless Controller delivering secure, reliable, and centrally managed wireless connectivity across all project locations.

a. The Access Points must support Wi-Fi 6, dual/tri-radio operation, 4×4 MIMO, high throughput across 2.4/5 GHz bands, multiple SSID modes (tunnel, bridge, split-tunnel, mesh), advanced wireless monitoring (rogue AP detection, WIPS/WIDS, spectrum analysis, packet sniffer), and seamless client experience features including load balancing, band steering, and channel optimization.

b. The APs shall integrate with the WBSEDCL's NAC-AAA and SD-WAN/NGFW systems for EAP-based authentication, dynamic VLAN assignment, CoA, posture enforcement, and identity-based access control. The Wi-Fi Controller shall be deployed fully on-premises, supporting high availability, up to 100 APs and 1,000 concurrent clients, multi-site centralized management, Wi-Fi 6/6E standards, mesh networking, QoS, guest access with captive portal, WPA2/WPA3 security, API/SNMP/Syslog integration, and full visibility into client sessions, RF parameters, and traffic usage.

c. The reporting and analytics framework shall provide real-time and historical Wi-Fi performance dashboards covering client connectivity, roaming, channel utilization, interference, coverage heatmaps, error/failure trends, throughput, application-level usage, RF health, firmware status, audit compliance, and wireless attack detection.

d. All features, performance parameters, RF capabilities, authentication functions, security controls, and reporting requirements shall fully comply with the detailed technical specifications defined in the Technical Annexures related to Wi-Fi Access Points, Wi-Fi Controller, and Wi-Fi Reporting.

96. Installation and Commissioning of Wi-Fi APs –

a. Perform setup, installation, commissioning, and integration of Wi-Fi Access Points and LAN cabling within the existing network at specified locations as per WBSEDCL's requirement in and around Kolkata.

b. Conduct a detailed site survey to identify optimal AP locations based on coverage, signal strength, interference, building layout, and network requirements.

c. Prepare and submit a detailed AP placement proposal, including a location map and technical justification for each AP position.

d. Ensure the proposal addresses aesthetic and practical considerations such as visibility, mounting feasibility, cabling routes, and equipment placement.

e. Submit the proposed plan to WBSEDCL for review and incorporate all feedback from WBSEDCL representatives before finalizing AP locations.

f. Carry out post-installation validation, including RF coverage testing, throughput checks, roaming verification, and performance benchmarking to confirm proper AP operation.

g. Implement strong security controls to safeguard the Wi-Fi infrastructure from unauthorized access, cyber threats, and data breaches.

h. Enable guest login through captive portal authentication using SMS-based OTP, email verification, and admin-group authorization workflows.

i. Enforce Layer-2 user isolation to prevent Wi-Fi users from accessing each other's devices or sessions.

j. Ensure that all Wi-Fi Access Points are updated with the latest stable firmware and security patches prior to final acceptance.

97. Network Racks- At sites where, existing network racks are already available, the bidder shall reorganize and properly mount the newly supplied SD-WAN devices and managed switches inside those racks. This includes the removal of old/legacy routers, switches, unused equipment, loose cabling, and non-standard installations, followed by proper placement of the new devices to ensure a clean, secure, and standards-compliant setup. The bidder shall provide all necessary accessories, including rack shelves, mounting kits, cable managers, patch cords, ties, power extension strips, and must ensure complete cleaning, dressing, and re-routing of cables for a professional rack layout.

98. For locations where, suitable racks are not available or are smaller than the required size, the bidder shall supply and install new 9U, 19-inch standard network racks as per project requirement. These racks shall securely house SD-WAN devices, 24-port managed switches, WAN link modems, power distribution units, and cable management components. The racks must support mounting of rackable equipment, shelf-based installation of non-rackable units, structured cable management through horizontal cable organizers, adequate ventilation with passive airflow and optional fan tray support, and must include a lockable front door and removable side panels for ease of maintenance. Each rack shall be supplied with a surge-protected internal power strip, grounding kit, M6 mounting hardware, blank panels, labeling provisions, and adequate internal depth for safe installation of SD-WAN and power equipment. All racks supplied or utilized shall fully comply with the technical requirements specified in the Technical Annexure related to the 9U Rack.

99. NOC Display-The bidder shall supply, install, configure and maintain the complete commercial-grade 4K displays (5 in no's) & Mini PC with wireless mouse and keyboard (5 in no's) setup including, heavy-duty stands (5 in no's), software, accessories and integrations. The supplied solution must ensure reliable multi-dashboard visibility for SD-WAN, Managed Switching, NAC-AAA, Log Servers and Reporting Analytics with smooth GUI performance over MPLS/LAN. All activities must comply with ISO 27001:2022 or latest controls (as applicable) and WBSEDCL security policies and shall fully comply with the technical requirements specified in the Technical Annexure related to NOC Displays and PCs.

SECTION: III

General Conditions of Contract [GCC]

GCC.1. Project Timeline:

The selected bidder shall conduct the POC/Acceptance Test upon receipt of the invitation letter. A timeline of 30 days shall be provided for completion of the POC, as defined in the Scope of Work. Upon successful completion of the POC, the LoA will be issued, and the subsequent timelines shall be adhered to as specified.

Sl. No	Milestone	Timeline
1	Placement of LOI/LOA	T0
2	LOA acceptance	T0 + 15 days
3	Deployment of a Network Architect for designing the Network Architecture and submitting the related documentation.	T0 + 30 days
4	Submission of PBG	T0 + 30 days
5	Kick of Meeting	After submission and review of the Network Architecture
6	Supply and delivery of SD-WAN boxes (B1, B2, B3), Wi-Fi controller, NAC-AAA, log server, reporting/analytics solution,Virtual Lab solution all Wi-Fi access , managed switches ,All NOC Display screen with stands , All PC with required accessories hardware, software, and licenses at DC, DR, Vidyut Bhavan, ALDC and Total: 50 nos. Type-A1 or A2 SDWAN boxes and 50 nos. Managed Switches, network rack at 50 site locations.	T0+ 90 days
7	Installation, integration of SD-WAN controller , Managed Switch controller, Wi-Fi controller, NAC-AAA, log server, reporting & analytics solution high-end SD-WAN boxes (Type-B1, Type-B2, and Type-B3) and all Managed Switches, Wi-Fi access points, along with all required hardware, software, and licenses at the respective locations— DC, DR, Vidyut Bhavan, and ALDC. Installation, integration SD-WAN boxes, managed switches network racks, NAC-AAA agents etc. with the relevant software and licenses – 50 Locations. Installation of Virtual Lab solution and basic configuration creation with connectivity establishments. Installation of NOC Screens and PC configurations with dashboards.	T0+ 120 days
8	Supply, delivery of SD-WAN boxes (Type-A1 or A2) and managed switches with the relevant software and licenses – another 300 Nos., along with network rack as per requirement.	T0+ 120 days
9	Supply, delivery of all devices or solutions in this project SD-WAN boxes (Type-A1 or A2) and managed switches with the relevant software and licenses along with network rack,as per requirement- remaining all locations,	T0+ 150 days
10	Installation, integration of all devices in this project, SD-WAN boxes, managed switches and Wi-Fi APs, network racks etc. with the relevant software and licenses at all locations. Tech spec and	T0+ 180 days

	related asset documentation, Virtual lab should be completely ready with as is configuration.	
11	**The Project Go-Live date shall be the date on which all devices/solutions are finally delivered, installed, configured, and all required documentation, license activations, and related activities are fully completed, which shall be considered as the start date of warranty/maintenance (Go-Live of the entire project) for the entire project.**	To be determined after completion of preceding milestone

Selected vendor will provide a detailed plan for all the activities (location wise) as per above timeline for the project and as mentioned in scope of work.

GCC.2. General Terms:

GCC.2.1. The entire project shall be executed on TURN KEY concept.

GCC.2.2. The bidder has to furnish all the information as required regarding their offer.

GCC.2.3. Quotation from any sub-vendor will not be entertained.

GCC.2.4. The bidder shall satisfy WBSEDCL with his ability to complete the works positively within the stipulated time.

GCC.2.5. The WBSEDCL reserves the right to reject the contract, even after placement of LoA, if any deviation from tendered specifications is found in at any point of time.

GCC.2.6. The Bidder should be capable of providing service throughout West Bengal.

GCC.2.7. If the vendor's performance of the work entrusted to it, is not found satisfactory in the contract period, WBSEDCL reserves the right to divide/split/modify/cancel the entire job without assigning any reason whatsoever.

GCC.2.8. All correspondence, documents and Bid, exchanged between the Bidder and WBSEDCL shall be written in English language. Failure to comply with this request may disqualify a bidder.

GCC.2.9. The Company reserves the right, to reject any or all the tenders, at its discretion, without assigning any reason whatsoever.

GCC.3. Variation:

The provisional quantity of the item is shown in the price schedule. WBSEDCL during execution of contract, reserves the right to increase or decrease the quantity of material +/- 25% of the quantity shown in the price schedule without any change in unit price or other terms and condition at the time of placement or during execution of work.

In addition to above, for Type-B1 SD-WAN Boxes deployed at DC and DR locations,

which are critical infrastructure components, WBSEDCL further reserves the right to procure additional quantities, up to a maximum of four (4) additional units over and above the originally indicated quantity, at the same unit price, commercial terms, and conditions as quoted in the Price Schedule, at any time during the contract period, based on operational, scalability, redundancy, or future expansion requirements.

GCC.4. Force Majeure :

GCC.4.1. WBSEDCL shall be under no liability if the vendor is prevented from carrying out any of the vendor's obligations by reason of war, Invasion, act of foreign country, hostilities, riots, civil commotion, mutiny, accident, earthquake, fires, floods, orders and / or restrictions and other cause beyond the reasonable control of the vendor. However, such force majeure circumstances are to be intimated immediately and to be established subsequently with proper documents / proofs to the entire satisfaction of WBSEDCL.

GCC.4.2. WBSEDCL will not take any additional liability towards enhanced taxes, duties and price variation due to force majeure condition.

GCC.5. Cancellation/Termination of Order:

WBSEDCL shall have the right to repudiate the contract if the work is not completed within schedule completion time as per "Project Timeline" Clause. The following causes may also lead to cancellation of LOA.

GCC.5.1. Non-acceptance of LOA as per "Acceptance" clause.
GCC.5.2. Non-submission of Performance BG within time.
GCC.5.3. If the performance of the work, entrusted to the awardee/contractor/vendor is not found satisfactory.
GCC.5.4. If the vendor fails to implement the project in time.
GCC.5.5. If the vendor is found to have "Conflict of Interest".

In each above cases 15 days' termination notice shall be issued prior to termination of LOA.

If the performance of the work entrusted to the successful bidder (L1) is found unsatisfactory and the order is terminated, the L2 bidder may be awarded the LOA for the said job, provided they agree to execute the work at the L1 rate and under the same terms and conditions. If the L2 bidder is unwilling or fails to execute the work, the next eligible bidder will be approached to carry out the job under the same terms and conditions.

GCC.6. Performance Guarantee:

GCC.6.1. As contract Performance Guarantee, the successful bidder has to furnish a Performance Guarantee in the form of Bank Guarantee on non-judicial stamp paper of Rs.100/- issued by any Scheduled Bank in India, as per format enclosed (ANNEXURE-V). The performance Guarantee security shall be submitted to the C.E., IT Cell, 3rd Floor, 'D' Block, Vidyut Bhawan, WBSEDCL. Performance BG amount is 10% of Total Contract Price excluding Taxes, to be submitted within 30 days from the date of issuance of LOA.

Validity of Performance Guarantee will be 6 years 6 months from the date of issuance of LOA and claim period will be further 3 months.

GCC.6.2. The Additional Performance Security shall be 100% of the unbalanced portion, i.e., where if the total value of the supply, delivery, and installation component of the contract price (excluding GST) exceeds 70% of the overall contract price (excluding GST).

Example- Total Bid : ₹10 Cr, 70% of bid amount = ₹7 Cr.
Total bid Warranty and Maintenance Support for all items = ₹1 crore
Total bid for Supply, delivery & installation for all items = ₹9 Cr, which exceeds 70% of bid amount i.e ₹7 Cr.
Unbalanced portion = ₹9 Cr – ₹7 Cr =₹2 Cr to be submitted as Additional BG

GCC.6.3. In addition to the Performance Security as mentioned above,

i) Additional Performance Security equal to 10% of the Total Contract Price (excluding taxes) shall be furnished, in the prescribed format, if the bid for items having variation of -20% to -50% of the estimated rate should be furnished in the prescribed format, within a period of 30 days from the date of issuance of LOA.

ii) Additional Performance Security equal to 20% of the Total Contract Price (excluding taxes) shall be furnished, in the prescribed format, if the bid for items having variation over -50% to -80% of the estimated rate should be furnished in the prescribed format, within a period of 30 days from the date of issuance of LOA.

Validity of all Performance Guarantees shall be 6 years and 6 months from the date of issuance of the LOA, with an additional claim period of 3 months.

GCC.6.4. Performance Guarantee is intended to secure the satisfactory performance by the contractor of the entire contract. However, it is to be construed as limiting the damages under contract period. No interest will be payable on Performance BG.

GCC.7. Way Leave (ROW):

Vendor shall arrange the necessary way leave for installation of any equipment in the office premises. It shall be the responsibility of the successful bidder, after awarded with the contract, shall have to arrange way leave/ROW (Right of Way) for installation of their equipment in connection to installation of SDWAN device/Switch. WBSEDCL shall neither negotiate with the owner of land/hired premises nor incur any additional charges towards obtaining way leave (ROW) permission whatsoever.

GCC.8. Legal Jurisdiction:

GCC.8.1. During execution of this contract, if any dispute arises thereby, shall be settled amicably between WBSEDCL and vendor to the extent possible.

GCC.8.2. Unresolved/unsettled disputes or differences shall be adjudicated only by the competent court of law under the jurisdiction of the Hon'ble High Court at Calcutta, if approached by either party. There shall not be any scope of initiation of arbitration proceedings for resolution of any dispute.

GCC.8.3. The necessary legal affairs and / or court case shall be exclusively within the jurisdiction of Calcutta High Court only.

GCC.9. Limitation of Liability:

Neither Party shall be liable to the other Party for any indirect or consequential loss or damage, loss of use, loss of production, or loss of profits or interest costs, provided that this exclusion shall not apply to any obligation of the bidder to pay liquidated damages to WBSEDCL, and

Except in cases of gross negligence or wilful misconduct, the aggregate liability of Bidder to WBSEDCL, whether under the Order, in tort, or otherwise, shall not exceed the amount specified in the Contract Price. Provided that this limitation shall not apply to the cost of repairing or replacing defective equipment/solutions with respect to patent infringement.

GCC.10. Liquidated Damage (LD):

The timely completion of entire project including handing over the sites to WBSEDCL as per "Project Timeline" is the basic consideration and essence of the contract and WBSEDCL reserves the right to repudiate the contract if vendor fails to complete the work within stipulated period for completion. However, the ordering authority may at its discretion waive this condition with imposition of liquidated damage indicated herein below:

GCC.10.1. **Delay in implementation of Project**: If the vendor fails to complete the work within the completion time as stated in the Clause of "Project Timeline", a L.D. (Liquidated Damage) @0.143% of the delivered/installation value for devices/solutions of the particular milestone offered beyond the stipulated timeline for each day of delay, subject to a maximum of 10% of the total contract value shall be imposed on the vendor.

As it is a turn-key project & mere provision of SDWAN devices cannot be construed as completion of work, hence for the purpose of this clause, work will be treated as finished only when successful installation, commissioning, POC and handover-takeover of the SDWAN devices is complete. Otherwise the work will be treated as unfinished and L.D. (Liquidated Damage) will be calculated on the line as mentioned above. L.D. (Liquidated Damage) if applicable will be deducted from the payment of milestone wise bill of the vendor.

GCC.10.2. Any liquidated damage, if involved under any of the aforementioned clauses, shall be realizable from any of the pending bills or Bank Guarantee given by the vendor lying with WBSEDCL.

GCC.11. Risk Purchase / Performance:

Adherence to time schedules mentioned in the foregoing clauses shall be deemed as the essence of contract and if the vendor performance of the work which entrusted to bidder is not found satisfactory of such work in the contract order, WBSEDCL shall be entitled to execute the job through the best and nearest substitute available elsewhere on the account and at the risk of the contracting agency or to cancel the

contract and the contracting agency shall be liable to compensate for any loss or damage which WBSEDCL may sustain by reason of such failure on the part of the Contracting Agency.

GCC.12. Service Level Agreement:

GCC.12.1. **Service/Device related**- The SLA shall apply in two conditions: (a) Major/Full Service or Device Down, where a device is non-functional or any major feature or service is unavailable, resulting in disruption of official work; and (b) Partial Service or Device Degradation, where the device remains operational but specific functions, ports, links, or services perform below acceptable levels. Failures arising from hardware faults, software issues, configuration errors, or license-related problems shall be treated as downtime or degradation, as applicable. All incidents—major or partial—shall be recorded in the WBSEDCL's incident reporting system and SLA calculations shall be based on these recorded incidents. The bidder's personnel will be given access to same. SLA will be imposed as per below table:

Sl. No	Location and device wise group	Allowed Time (Major/Full Down)	Penalty (Major/Full Down)	Allowed Time (Partial Service)	Penalty (Partial Service
1	**DC, DR, VB, ALDC** (SDWAN Controller, boxes, Switch Controller, switch, WiFi Controller, NAC-AAA, Log Server, Reporting Analytics, WiFi Aps, Virtual Lab., NOC display system.) Applicable if any device or its key functionality is unavailable	2 hours	Nil	24 hours	Nil
		More than 2 hours	Rs. 2000/- will be deducted per hour of delay	More than 24 hours	Rs. 200/- will be deducted per hour of delay
2	**Site office** (SDWAN box, switches). Applicable if any device or its key functionality is unavailable	24 hours	Nil	24 hours	Nil
		More than 24 hours	Rs. 500/- will be deducted per hour of delay	More than 48 hours	Rs 100/- will be deducted per hour of delay
3	**Hill area Site office under Siliguri Zone** (SDWAN box, switches). Applicable if any device	48 hours	Nil	48 hours	Nil

	or its key functionality is unavailable. Districts-Darjeeling,Kalimpong,Jalpiguri,Alipurduar,Coochbehar.	More than 48 hours	Rs. 500/- will be deducted per hour of delay	More than 48 hours	Rs. 100/- will be deducted per hour of delay

FULL / MAJOR SERVICE OR DEVICE DOWN

- Complete hardware failure of devices supplied under this project (SD-WAN boxes, L2 switches, Switch Controller, Wi-Fi Controller/APs, NAC/AAA, Log Server, Reporting and analytics systems, Virtual Lab., NOC display system).
- Major software/firmware failure or corruption causing device unavailability.
- License failure preventing device operation.
- Loss of critical network connectivity making official applications inaccessible.
- Failure of NAC/AAA causing authentication blockage.
- Controller or Log/Reporting system completely unavailable.
- If the issue affects only one site, it is treated as Full Down – Site Office.
- If the issue affects multiple sites or central systems, it is treated as Full Down – DC/DR.

PARTIAL SERVICE DEGRADATION

- Port failure, degraded throughput, or limited connectivity.
- Minor component failure without complete outage.
- Delayed or failed alerts, dashboards, or monitoring.
- Reporting/analytics module issues or partial log ingestion failure.
- Controller module/function failure (template push, profiles, visibility, etc.).
- Patch/backup/API issues.
- If issue affects only a particular site, treated as Partial – Site Office.
- If issue affects central systems, treated as Partial – DC/DR.

DOWNTIME NOT ATTRIBUTABLE TO THE BIDDER

- Power outage.
- ISP/MPLS/Internet link failure.

TECHNICAL SPECIFICATION COMPLIANCE (FULL OR PARTIAL CLASSIFICATION)

- Any feature specified in the Technical Specifications / Annexures and Scope of Work must be fully delivered and functional throughout the project period.
- If the missing or malfunctioning feature during project period causes limited impact, it is classified as Partial Service Degradation.
- If it results in complete service/device failure or inability to perform official work, it is classified as Full/Major Down.
- This classification applies in addition to Full and Partial definitions for SLA enforcement.

GCC.12.2. **Preventive Maintenance**-If If the Vendor fails to complete the scheduled Preventive Maintenance (PM) within the stipulated timeline (i.e., every six months from the date of issuance of the LoA), the following penalty shall be applicable:

(a) Site Offices-In case of non-completion of PM at Site Offices, a penalty/deduction of 10% of the total quoted price of the respective devices, i.e., SD-WAN Router and Managed Switch, including Supply, Delivery, Installation, and Warranty/Maintenance charges, shall be imposed for the affected site. A PM shall be considered complete as per process and steps mentioned latter.

(b) DC / DR /VB/ALDC (Central Locations)-

In case of non-completion of PM at Central locations, a penalty/deduction of 10% of the total quoted price of the corresponding devices deployed at the location, including Supply, Delivery, Installation, and Warranty/Maintenance charges, shall be imposed .

If a minimum gap of 120 days is not maintained between two successive PMs, the PM claimed for that billing cycle shall be treated as "Not Done", and a penalty/deduction of 10% of the total quoted price of the respective device, as stated above, shall be imposed.

The PM cycle shall commence from the Go-Live date, and a total of ten (10) Preventive Maintenance cycles must be completed during the entire project period. Since each PM is performed every six (6) months, any SLA penalties arising from missed, delayed, or incomplete PM activities will be deducted from every warranty/maintenance bills. The Bidder shall therefore ensure timely submission of all PM hardcopy certificates along with the consolidated summary Excel report for each completed PM cycle.

A PM will be considered as "Completed" only when all tasks assigned under the PM Scope of Work are fully carried out. This includes, but is not limited to:

- Device-level checks and maintenance, configuration reviews and reporting
- NAC-AAA agent verification/TLS/SSL inspection verification and survey,
- Reporting/observations submission,
- Compliance checks as defined in the PM checklist.

If any mandatory PM task remains incomplete or unattended, the PM for that site shall be treated as "Not Done", irrespective of site visit, and penalties shall apply accordingly as mentioned above. A PM format or report will be given by WBSEDCL during LOA placement which needs to be followed by bidder.

GCC.12.3. **Manpower related:** L2 onsite personnel deployed at DC/DR/VB must remain physically present during assigned duty hours and report to the WBSEDCL's Controlling Officer or designated official.

Any unapproved absence, non-presence during duty hours, or failure to attend responsibilities will attract a penalty of ₹2,000 per day per personnel, deducted from the half yearly service & maintenance bill.

GCC.12.4. The cumulative penalty (including SLA, Preventive Maintenance, and Manpower-related penalties) for any given half-year period shall not exceed **25% of the corresponding half-yearly contract value**. If the penalty imposed on the selected bidder exceeds 25% of the half yearly bill amount in two consecutive half year, WBSEDCL may choose to terminate the contract and forfeit the security deposit submitted by the selected bidder. WBSEDCL may

deem this event to be an event of "default" leading to possible termination of the contract. In such a case, if WBSEDCL decides to terminate the contract, the selected bidder will be given 30 days to close the contract.

GCC.12.5. The SLA shall be applicable on a 24×7×365 basis. SLA related calculation will be based on WBSEDCL incident management system. All devices and services covered under this SLA are expected to remain operational at all times, and downtime or degradation—whether occurring during working hours, non-working hours, weekends, or holidays—shall be measured continuously without any exclusion window.

GCC.13. Terms of Payment:

GCC.13.1. The payment will be made for supply, delivery, installation and FMS on below milestone basis.

Supply and Delivery

Sl. No.	Milestone	Activity	Timeline	Payment % of Contract Price
1	M1	Supply, delivery of high-end SD-WAN boxes (Type-B1, Type-B2, and Type-B3), Wi-Fi controller, NAC-AAA, log server, reporting and analytics solution, Virtual Lab solution ,all Wi-Fi access points, All NOC Display screens with stand,All PC along with all required accessories, hardware, software, and licenses at the respective locations — DC, DR, Vidyut Bhavan, and ALDC.L2,L3,SPOC assigned personnel details.	90 days from LOA	20
		Supply, delivery of SD-WAN boxes(Type-A1/A2) ,managed switches with the relevant software and licenses and Network rack – 50 Nos.		
2	M2	Supply, delivery of SD-WAN boxes (Type-A1/A2), managed switches with the relevant software and licenses and Network rack – another 300 Nos.	120 days from LOA	15
3	M3	Supply, delivery of all devices or solutions in this project - SD-WAN boxes (Type-A1/A2) and managed switches with the relevant software and licenses along with network rack as per requirement- remaining all locations,	150 days from LOA	15

Service: Installation/Implementation, Integration.

6	M4	Installation, integration of high-end SD-WAN boxes (Type-B1, Type-B2, and Type-B3), all controllers, NAC-AAA, log server, reporting and analytics solution, and all Wi-Fi access points, along with all required hardware, software, and licenses at the respective locations— DC, DR, Vidyut Bhavan, and ALDC. Installation of Virtual Lab solution and basic configuration creation with connectivity establishments. Installation of NOC Screens and PC configurations with dashboards.	120 days from LOA	10
		Installation, integration of SD-WAN boxes , managed switches, NAC-AAA agents with the relevant software and licenses – 50 Nos.	120 days from LOA	
7	M5	Installation, integration of all devices and solutions in this project- SD-WAN boxes, managed switches, NAC-AAA agents with the relevant software and licenses etc. – All remaining locations. Tech spec and related asset documentation-. Virtual lab should be completely ready with as is configuration.	180 days from LOA	10
FMS -5 years of post–go-live warranty and maintenance support				
9	M6	Maintenance of the entire project 3% per half yearly basis at the end of particular half year against the bills submitted by bidder after providing satisfactory service for the bill period.	5 Years (10 Half Year) from date of maintenance start date	30

GCC.13.2. Payment of first bill will be released after submission of PBG and supply, delivery and installation certificate of newly installed sites signed by the respective site of WBSEDCL, which shall be provided along with the bill.

GCC.13.3. In case of delay in supply, delivery and installation payment shall be made after deducting LD as applicable.

GCC.13.4. Payment for FMS support shall be made half yearly from the Go-Live date of the respective milestone, based on submission of the call details report and the PM details report and other asked reports or certificates.

GCC.13.5. A Satisfactory Training Completion Certificate must be submitted, along with the details of the training conducted, as specified in the Scope of Work along with First FMS bill.

GCC.13.6. Submission of the Final Master Documentation Package (as per the Technical Annexure) along with the first FMS bill, followed by yearly submission of the revised and updated documentation package with subsequent FMS bills in accordance with schedule.

GCC.13.7. In case of any delay in support services, PM services, or absence of manpower, the payment shall be made after deducting the applicable SLA penalties.

GCC.13.8. Payment for subsequent half year will be made only after payment of previous half year.

GCC.13.9. All the bills in triplicate with relevant papers, documents are to be submitted to the Controlling Officer at IT Cell for payment.

GCC.13.10. If you fail to submit normal/final bills prior to two months of expiry of PBG in consideration to the validity period of the PBG, the said PBG shall be invoked by WBSEDCL without further reference.

GCC.14. WBSEDCL personnel for liaison:

GCC.14.1. **Controlling Officer:** Additional Chief Engineer, IT Cell. – He/She would issue the successful completion certificate.

GCC.14.2. **Nodal Officer:** Superintending/Divisional/Assistant Engineer, IT Cell – He would supervise & monitor all the activities.

GCC.14.3. **Site Officer :** Concern Site incharge of respective sites.

GCC.14.4. **Paying Authority:** Manager(F&A), IT Cell, Vidyut Bhavan,WBSEDCL.

Acronyms and Full Forms

AAA – Authentication, Authorization and Accounting
AD – Active Directory
AES – Advanced Encryption Standard
ALDC – Area Load Dispatch Centre
API – Application Programming Interface
AP – Access Point
BOQ – Bill of Quantities
BCP – Business Continuity Plan
CAPA – Corrective and Preventive Actions
CCC – Customer Care Centre
CERT-In – Indian Computer Emergency Response Team
CLI – Command-Line Interface
CoA – Change of Authorization
CPU – Central Processing Unit
CR – Change Request
CPE – Customer Premises Equipment
DC – Data Centre
DHCP – Dynamic Host Configuration Protocol
DNS – Domain Name System
DR – Disaster Recovery
DRC – Disaster Recovery Centre
EAP – Extensible Authentication Protocol
EOL – End of Life
EOS – End of Support
EDR – Endpoint Detection and Response
EVE-NG – Emulated Virtual Environment – Next Generation
FW – Firewall
GUI – Graphical User Interface
HA – High Availability
HLD – High-Level Design
HQ – Head Quarters
HTTP – Hypertext Transfer Protocol
HTTPS – Hypertext Transfer Protocol Secure
IDS – Intrusion Detection System
IGMP – Internet Group Management Protocol
ILL – Internet Leased Line
IOCs – Indicators of Compromise
IP – Internet Protocol
IPAM – IP Address Management
IPS – Intrusion Prevention System
IVRS – Interactive Voice Response System
LAN – Local Area Network
LDAPS – Lightweight Directory Access Protocol Secure
LLD – Low-Level Design
LACP – Link Aggregation Control Protocol
MAF – Manufacturer Authorization Form
MAC – Media Access Control
MPLS – Multi-Protocol Label Switching
MTBF – Mean Time Between Failures
MTTR – Mean Time To Repair

NAC – Network Access Control
NAT – Network Address Translation
NAT-T – NAT Traversal
NCIIPC – National Critical Information Infrastructure Protection Centre
NGFW – Next-Generation Firewall
NMS – Network Management System
NTP – Network Time Protocol
OEM – Original Equipment Manufacturer
OS – Operating System
OTP – One-Time Password
PC – Personal Computer
PM – Preventive Maintenance
POC – Proof of Concept
PRI – Primary Rate Interface
QoS – Quality of Service
RAID – Redundant Array of Independent Disks
RBAC – Role-Based Access Control
RCA – Root Cause Analysis
RFP – Request for Proposal
RF – Radio Frequency
REST API – Representational State Transfer – Application Programming Interface
SDWAN-Software-Defined Wide Area Network
SFP – Small Form-Factor Pluggable
SIEM – Security Information and Event Management
SIP – Session Initiation Protocol
SLA – Service Level Agreement
SNMP – Simple Network Management Protocol
SNR – Signal-to-Noise Ratio
SOP – Standard Operating Procedure
SSL – Secure Sockets Layer
STP – Spanning Tree Protocol
TAC – Technical Assistance Center
TLS – Transport Layer Security
UDP – User Datagram Protocol
TCP – Transmission Control Protocol
URL – Uniform Resource Locator
VC – Video Conferencing
VLAN – Virtual Local Area Network
VM – Virtual Machine
VPN – Virtual Private Network
VRF – Virtual Routing and Forwarding
WAN – Wide Area Network
WLAN – Wireless Local Area Network
WIPS – Wireless Intrusion Prevention System
WIDS – Wireless Intrusion Detection System
ZTNA – Zero Trust Network Access

Technical Annexures (T-1 to T-14)

Note 1: Technical Annexures (Annexure T-1 to T-10) shall be jointly signed and stamped by the Bidder/System Integrator and the respective OEM(s) for the products being supplied.

For clarity and uniformity, the Bidder/System Integrator shall sign, seal, and stamp on the left-hand side of each page, and the respective OEM shall sign**,** seal, and stamp on the right-hand side of each page of the applicable annexures.

Technical Annexures (Annexure T-11 to T-14) – To be signed and stamped by the Bidder/System Integrator.

OEM Declaration**:**

By signing the relevant Technical Annexures, the respective OEM(s) confirm that the proposed products and solutions fully comply with the stated technical specifications, functional requirements, security capabilities, and certifications as mentioned in the tender. The OEM further confirms that the proposed hardware and software products shall remain available, supported, and maintainable for the entire project duration. This confirmation is strictly limited to OEM product capabilities, specifications, licensing, and support, and shall not extend to deployment, integration, configuration, operations, or service delivery, which shall remain the sole responsibility of the Bidder/System Integrator.

Bidder / System Integrator Declaration**:**

By signing these annexures, the Bidder/System Integrator accepts full responsibility for all implementation, integration, configuration, commissioning, operations, support, supply of accessories, and all project deliverables throughout the project period. The Bidder/System Integrator shall ensure correct deployment, configuration, and lifecycle management of all OEM-provided features, specifications, and technologies during the entire project duration.

Note 2 : If any compliance requirement specified for a solution component is fulfilled through another integrated component, the Bidder/System Integrator shall clearly indicate the same as “Complied through <Component Name>” in the relevant annexure remarks column.

Such cross-component compliance shall be subject to review and acceptance by WBSEDCL and the Bidder/System Integrator shall remain fully responsible for ensuring end-to-end compliance.

Example:
If a reporting or analytics requirement listed under the Report & Analytics Annexure is fulfilled through the SD-WAN Controller, it shall be mentioned as “Complied through SD-WAN Controller.” In Remarks column.

Annexure-T-1

Network & Security Device – General Compliance Requirements:

T1 Annexure is applicable only to OEMs of the following devices and solutions proposed under this project - SD-WAN edge devices and controllers, Managed Network Switches and Controller, Wi-Fi Access Points and Wireless Controllers, Network Access Control (NAC) systems, Authentication/Authorization/Accounting (AAA) systems, Log Management Servers, and Reporting / Analytics Dashboard platforms.

Where products from multiple OEMs are proposed, a separate T1 Annexure shall be submitted for each respective OEM signed by both OEM and bidder, covering only the devices and solutions supplied by that OEM. For same OEM just mention the device names clearly.

"NA" (Not Applicable) may be used only where the requirement is genuinely not applicable to the device category. The reason for marking NA shall be clearly described in the Remarks column. All NA entries are subject to review and final acceptance by the Organization (WBSEDCL).

Device/Product/Solution Name for which T1 being submitted-

Sl. No.	Requirement and Compliances	Yes / No	Remarks
	Compliance, Governance & OEM Obligations-		
1	All network-connected devices that require IP addressing must support both IPv4 and IPv6 and provide full dual-stack (IPv4/IPv6) capability, configurable as per WBSEDCL requirements. The solution shall ensure seamless operation in mixed IPv4/IPv6 environments, support future readiness for IPv6-based services, and handle all industry-standard IPv6 packet types, protocols, and routing mechanisms.		
2	The OEM confirms compliance with secure supply chain practices and Secure Development Lifecycle (SDL/SSDLC) processes, ensuring that the proposed hardware and software components are developed, sourced, and maintained in accordance with security best practices and are free from banned, embargoed, or high-risk country-of-origin concerns, in line with Government of India guidelines.		
3	The proposed solution must be a commercially supported, enterprise-grade product and shall not include any open-source, community edition, trial, or unsupported variant.		
4	All devices and solutions must be deployed on-premises, and no WBSEDCL data shall be transmitted or stored outside WBSEDCL's environment. However, patch and security updates from OEMs are permitted, provided they do not result in data being transferred off WBSEDCL's environment.		

5	All proposed hardware and software products must be currently in production and not declared End-of-Sale at the time of delivery. The OEM must additionally commit that none of the proposed products will reach End-of-Support (EoS) for a minimum of five (5) years from the Project Go-Live Date (Zero Date).		
6	OEM must have **a** responsible disclosure process and a time-bound patch release SLA for critical CVEs (Common Vulnerabilities and Exposures).		
7	The bidder must submit a valid and original Manufacturer Authorization Form (MAF) from the respective OEM for each and every hardware device, software component, controller, appliance, and solution proposed in this project.		
	Security, Access Control & Hardening-		
8	All devices and systems that provide administrative login interfaces must support Role-Based Access Control (RBAC) and Multi-Factor Authentication (MFA). via sms/email.		
9	All active network devices, **where applicable**, shall support Secure Boot and firmware integrity validation to ensure that only OEM/vendor-signed firmware is executed. Devices must reject and log any unauthorized, tampered, or corrupted firmware images. All firmware upgrades, patches, and updates shall be verified through checksum and/or OEM-recommended digital signature validation prior to installation.		
10	The OEM shall provide security hardening guides for all proposed devices and systems, such as STIGs, CIS Benchmarks, or OEM-validated best-practice configurations during installation and configuration. These guides shall be used by the System Integrator for configuration validation and implementation during deployment.		
11	All devices shall support secure management, monitoring, authentication, logging, and time synchronization using industry-standard protocols such as SSH, TLS-based services, SNMP, encrypted logging, and secure NTP, implemented using the latest secure protocol versions. (where applicable), and integration with centralized AAA (RADIUS,TACACS+) backed by integration with centralized directory services (LDAPS,LDAP,AD) with full audit logging, session control, and protocol hardening.		
12	Remote or VPN-based administrative access is discouraged and shall be permitted only in **exceptional cases** where specialized support is required, and only after obtaining prior written approval from WBSEDCL and as per WBSEDCL's Remote connection policy.		
13	All devices with administrative or user login interfaces must support configurable login banners for security notices, legal disclaimers, and authorized-use statements.		

14	All devices with administrative interfaces must support integration with industry-standard Privileged Identity/Access Management (PIM/PAM) solutions (**bidder will not have to provide PIM/PAM solution in this project**) and approval-based privileged access, using RADIUS, TACACS+, backed by integration with centralized directory services (LDAP, LDAPS, AD) or REST API-based methods as applicable.		
15	**Where applicable**, devices and systems shall support centralized certificate lifecycle management (issuance, renewal, revocation, expiry) and integration with an approved OEM-managed or Enterprise CA. Any required PKI/CA shall be provided and managed by the Bidder/System Integrator		
16	Devices in the project must support integration with the WBSDCL's NTP server to ensure accurate time synchronization, so that log timestamps and all time-sensitive records are maintained securely and consistently across the entire infrastructure.		
	Logging, Monitoring & SIEM Integration-		
17	All network and security devices that generate audit, security, or operational logs—must support industry-standard log formats such as Syslog RFC 5424 and CEF (where applicable), and must transmit logs securely to the centralized Log Server or SIEM using encrypted channels such as Syslog over TLS or HTTPS-based log APIs. All such devices must be fully **integrated** with the WBSEDCL's SIEM/SOC platform for centralized log collection, correlation, monitoring, and compliance reporting, ensuring confidentiality, integrity, and reliable delivery of logs.		
18	The Bidder shall ensure that security, access, and critical operational logs from all project devices and platforms are retained for a minimum of 180 days.		
	Architecture, High Availability & Implementation Support-		
19	The proposed solution must be fully supported by the OEM/vendor with valid enterprise licensing and support entitlements. The OEM/vendor shall provide: (a) Annual Technical Support (ATS), including software updates, security patches, and bug-fix releases. (b) Facility Management Services (FMS), as applicable, for on-site operational assistance and issue resolution. (c) Access to a 24×7 OEM Technical Support Centre or equivalent helpdesk for incident reporting and technical escalation		
20	Controllers, high-end devices, servers, and software solutions provided under this project—including SD-WAN controllers, high-end SD-WAN devices, Switch controllers, NAC, AAA, log servers, and reporting/analytics platforms—must support deployment in Active-Active or Active-Passive mode (as applicable), with one instance at the Data Centre (DC) and the corresponding instance at the Disaster Recovery (DR) site to ensure high availability and continuity. This requirement excludes site-level SD-WAN edge devices, site-level managed switches, and Wi-Fi access points.		

Annexure-T-2

Section A .SD-WAN Device Technical & Functional Requirements-

(SD-WAN Device Common Requirements Applicable to all SD-WAN devices in this project)

Sl. No	Technical & Functional requirements	Compliance(Yes/ No	Remarks
	SD-WAN Architecture & WAN Connectivity-		
1	All components of the proposed SD-WAN solution must be deployed on-premises.		
2	SD-WAN devices must operate under a true Software-Defined Network (SDN) architecture, with centralized control/management hosted in the SD-WAN Controller/Manager/Orchestrator. It must provide logical separation of control, management, and data planes, and support integration of various underlay links (MPLS, ILL, Broadband etc) using policies.		
3	SD-WAN devices must support simultaneous connectivity to multiple WAN transports (MPLS, ILL, Broadband, etc.) and establish encrypted overlay tunnels in active-active mode with intelligent load balancing and automatic failover based on real-time link performance (latency, jitter, packet loss).		
4	SD-WAN devices must support enterprise routing protocols including Static Routing, OSPF v2/v3, iBGP, eBGP, route redistribution, filtering, and summarization.		
5	The SD-WAN solution (device in coordination with controller) should offer flexible architectures including Hub-to-Spoke (partial mesh), Spoke-to-Spoke (dynamic full mesh or via DC/DR), Multi-Hub, Multi-Region, and support for DIA (Direct Internet Access) / RIA (Remote Internet Access) for the branches.		
6	SD-WAN devices must support advanced traffic control features such as Application-Aware Routing (via DPI/signatures), Policy-Based Routing, SLA-aware routing, WAN load balancing, per-application steering, and automatic fall-back based on link health.		
	Application, Performance & QoS-		
7	SD-WAN devices must support enterprise-grade QoS including traffic classification, DSCP/TOS marking, rate-limiting/policing, traffic scheduling (e.g., WFQ, priority queuing), application-based queuing, and interface-level QoS enforcement per WAN link.		

	In addition, devices must support Diff Serv-based and device-level queuing mechanisms to ensure consistent traffic prioritization and SLA adherence even under congestion or across multiple WAN links.		
8	SD-WAN devices must support Deep Packet Inspection (DPI) to detect and classify applications (e.g., O365, Google Workspace etc) and enforce application-level routing, QoS, and security. It must maintain an on-prem application signature database with automatic or manual updates.		
9	SD-WAN devices must allow creation of custom application signatures using IP, port, domain/FQDN, URL patterns, or protocol behaviour. These signatures must support routing, QoS, security, and application-based steering for enterprise or internal applications		
10	Must support application-level monitoring and enforcement of QoS parameters, including metrics such as MOS (Mean Opinion Score) or OEM-defined classification, jitter, latency, and packet loss—particularly for real-time applications (e.g., VoIP, video conferencing). It must also enable automatic failover or path switching when these thresholds are breached, and provide both live dashboards and historical reporting for performance analysis.		
11	Must support real-time path monitoring with dynamic path selection, active-active or active-standby forwarding, without session drops to ensure uninterrupted service continuity.		
12	The SD-WAN must support identity-based policy enforcement using user/group information obtained NAC/AAA systems backed by integration with directory services (Active Directory (AD) ,LDAP,LDAPS). Policies must support per-group (user id based) routing, QoS, and access control to enable Zero Trust behaviour (e.g., different WAN paths or priorities based on user role).		
13	The SD-WAN devices must support REST APIs for automation, orchestration, and integration with NMS/SIEM systems. Devices must transmit complete and unaltered log data directly to SIEM or via the central log server as required.		
14	In headless mode, devices must continue forwarding data even without connectivity to the controller/orchestrator.		
15	The SDWAN devices shall support application-aware traffic steering for IPv6, enabling identification of IPv6-based applications and enforcing routing, QoS, security, and access policies analogous to IPv4. It must ensure seamless operation in dual-stack environments and be fully capable of supporting modern IPv6-based services, cloud applications, and future network expansions.		
	Network Services, NAT, L2/L3 & Segmentation		
16	Devices must provide a dedicated console or management port (physical or logical) for secure out-of-band management, while also supporting in-band management via WAN links for controller communication.		

17	The SD-WAN devices must support multiple NAT modes including static NAT (one-to-one) and dynamic NAT/PAT (many-to-one) for flexible and secure internet access.		
18	The SD-WAN devices must support NAT Traversal (NAT-T) to ensure the seamless establishment of overlay tunnels (e.g., IPsec, GRE, VXLAN) from devices located behind NAT-performing routers or firewalls.		
19	Devices must support secure boot and cryptographic firmware validation to ensure software integrity during the boot process, to prevent the execution of tampered firmware, malware, rootkits, or backdoors during the earliest stages of device operation.		
20	The SD-WAN devices must support required Layer 2 and Layer 3 features including VLAN tagging (802.1Q), trunking, LACP, virtual interfaces, and related managed-switch features. They must interoperate fully with managed switches, NAC, AAA, and DHCP systems without limiting any enterprise functionality.		
21	The device must support Virtual Routing and Forwarding (VRF) or equivalent for logical separation of MPLS, Internet, and Management traffic. Each VRF must support independent firewall, NAT, and QoS policies. The solution must also support route leaking with full policy enforcement where selective sharing of routes is required.		
22	SD-WAN devices must support Bidirectional Forwarding Detection (BFD) or an equivalent fast-failure detection mechanism for rapid detection of path failures		
	Device Lifecycle, Uniformity & Security Compliance		
23	SD-WAN devices must support granular intra-subnet traffic control, enabling per-group (user id based), per-device, and per-application policy enforcement. Identity-based policies must be supported through integration with NAC,AAA, backed by integration with centralized directory services (AD,LDAP,LDAPS). Optional IP or IP-segment-based policies may be used only for unmanaged devices such as IoT, printers, CCTV, or guest networks.		
24	SD-WAN devices must support centralized and automated deployment of firmware, security patches, and signature updates from the SD-WAN controller. Updates must support per-device, per-group, and bulk scheduling, with integrity verification and version control.		
25	SD-WAN devices belonging to the same device category (e.g., Type A, Type B, Type C, Type D) shall be of the same hardware model, run the same OS version, and possess identical license features to ensure uniform functionality, interoperability, and ease of maintenance.		
26	SD-WAN devices shall provide secure storage of cryptographic keys and device identity credentials using a Trusted Platform Module (TPM 2.0) or an equivalent hardware or firmware based trusted security element. Devices shall support industry-standard encryption and key-exchange algorithms as part of secure protocols. The OEM shall furnish product datasheets or official compliance statements confirming the presence		

	and functionality of the TPM 2.0 or equivalent trusted security module in the proposed devices.		
27	SD-WAN devices must use certificate-based mutual authentication with the SD-WAN controller, with each device provisioned with a unique X.509 certificate issued by the approved Certificate Authority (OEM CA or an Enterprise on-premises CA). The Bidder shall be responsible for secure CSR generation, certificate issuance, deployment, renewal, and revocation throughout the project lifecycle. If an Enterprise CA or OEM CA is proposed, the Bidder shall supply, deploy, and fully maintain all required components—including hardware, software, licenses, HSM (optional), and subscription/support costs—ensuring complete PKI functionality and compliance with the approved CA hierarchy and security policies.		
28	SD-WAN devices must support TLS/SSL inspection using an approved Root/Intermediate CA. The Bidder must ensure trusted certificate deployment to all endpoints through centralized or manual methods. The SD-WAN must support selective encrypted-traffic inspection, exemption of internal traffic, and full PKI lifecycle management.		
29	The SD-WAN devices must support fully selective, policy-driven TLS/SSL inspection. Inspection shall be completely disabled by default and may be enabled only for Internet-bound and/or Intranet-bound traffic strictly as per the WBSEDCL's security policy. The inspection engine must allow granular bypass based on application category, domain/FQDN, URL category, user/group identity, or regulatory requirements. Mandatory exemptions must be enforced for banking, financial, government, privacy-sensitive, or any other restricted traffic categories in accordance with RBI, CERT-In, MeitY, and WBSEDCL's security guidelines. TLS/SSL inspection shall apply only to explicitly approved traffic flows.		
30	The proposed SD-WAN devices shall be Common Criteria evaluated/certified under relevant Protection Profiles (such as NDPP, Stateful Traffic Filter Firewall, IPS, SSH, VPN Gateway). The certification may apply to either the hardware appliance or the software/virtual image, as officially certified by a CCRA-recognized scheme or an Indian CCTL laboratory (STQC/MeitY). The OEM shall provide evidence of certification and ensure that certified firmware/software images are made available and supported for the supplied devices.		
31	The SD-WAN devices shall use cryptographic modules compliant with internationally recognized security standards—such as FIPS 140-2/140-3 (Level 2 or higher), / certifications issued by Government of India approved laboratories,/ any equivalent international certification validating the secure functioning of cryptographic modules/The OEM shall provide an undertaking confirming that all cryptographic and		

	security functions will operate securely and remain compliant with the relevant international standards throughout the entire project period.		
32	The SD-WAN devices under this project shall comply with internationally recognized IPv6 standards, such as the IPv6 Ready Logo or any equivalent certification issued by an accredited IPv6 testing laboratory / Government of India–approved lab reports demonstrating full conformity with industry-standard IPv6 features /The OEM shall provide an undertaking confirming that the device possesses one of the above certifications or an equivalent certification (with supporting details), and that all required IPv6 features and functionalities will function fully, reliably, securely and as per relevant international standards throughout the project period.		
33	SD-WAN devices must support **DHCP Server** functionality for assigning and managing IP addresses for endpoints such as PCs, printers, CCTV cameras, biometric terminals, and IoT devices, ensuring reliable and conflict-free IP allocation.		
	Branch Network Services & Threat Intelligence-		
34	SD-WAN devices must support **DHCP IP Reservation** based on client MAC address to ensure consistent IP assignment across device reboots, OS reinstalls, or hardware replacement.		
35	The SD-WAN devices proposed under this project shall be fully interoperable and compatible with the managed switches being provided, and shall operate seamlessly with all Layer-2 and Layer-3 security and control features mandated for those switches under this project.		
36	The SD-WAN box must support or forward DHCP Option 66 and 67 (or equivalent OEM protocols) to enable PXE boot and IP phone provisioning. Eg . A new VoIP phone plugged into the network receives an IP from DHCP, then uses Option 66/equivalent to locate the TFTP server and Option 67/equivalent to download its config.		
37	SD-WAN devices must support or forward DHCP Option 43/equivalent for vendor-specific information (e.g., WLAN controller discovery for APs) and DHCP Option 82/equivqlent for relay agent information insertion (e.g., circuit ID, switch port ID) to support NAC, VLAN assignments, and port-level user tracking.		
38	SD-WAN devices must log all DHCP transactions with timestamp, assigned IP, and client MAC address in log server. These logs must be exportable via Syslog or SNMP to central log collectors or SIEM systems.		

39	The SD-WAN device must support coordination with the WBSEDCL's DNS infrastructure and transparently redirect all endpoint DNS queries to the designated internal/external DNS servers located at DC and DR. The device must support DNS forwarding, split DNS, and policy-based DNS assignment. After resolution: **Internal/intranet domains** must be routed through SD-WAN overlay tunnels to the internal network (DC/DR). **External/internet domains** must be routed through local internet breakout at the site SD-WAN device, subject to defined security checks (firewall, URL filtering, IPS, etc.).		
40	Must provide local DNS caching preferably and configurable fail-open/fail-close policies to maintain user experience in case of temporary unreachability of DC/DR DNS servers.		
41	The SD-WAN devices must support integration with WBSEDCL's Threat Intelligence (TI) server or sources—either directly or through the SD-WAN controllers—**using API-based or middleware connectors**. Any additional hardware, software, or licenses required for such integration shall be provided by the Bidder. The solution must support ingestion and validation of network-related Indicators of Compromise (IOCs), including but not limited to malicious IP addresses, domains, URLs, and other SD-WAN-relevant threat indicators. After IOC ingestion and validation, the SD-WAN devices shall ensure that all allowed traffic undergoes local security inspection (e.g., firewall, URL filtering, IPS/IDS), while malicious or IOC-matched traffic is blocked, quarantined, or redirected as per WBSEDCL's security policies.		

Section B. Site-End SD-WAN Device Specifications and Additional Requirements

Applicable Device Categories:

- **Type-A1** -692 nos. boxes (around 30-50 users/devices)
- **Type-A2-**50 nos. boxes (approx. 200-300 users/devices)

1	The SD-WAN site device must comply with all capabilities defined under Section A (SD-WAN Device Technical & Functional Requirements) to ensure secure, reliable, and seamless network connectivity at each branch location.		

2	**The Type A1 SD-WAN site device must have:** 1. **A minimum of 6 × 1G RJ45 Ethernet ports that are configurable and may be assigned as either WAN or LAN interfaces as per WBSEDCL's requirements.** OR **A minimum of 4 × 1G RJ45 Ethernet WAN ports AND A minimum of 4 × 1G RJ45 Ethernet LAN ports as per WBSEDCL's requirements.** 2. **Minimum 200 Mbps of sustained SD-WAN throughput** with all features enabled, including DPI, NGFW, IPS/IDS, and TLS/SSL inspection, as defined in Section A and Section B.		
3	**The Type A2 SD-WAN site device must have:** 1. **A minimum of 6 × 1G RJ45 Ethernet ports that are configurable and may be assigned as either WAN or LAN interfaces as per WBSEDCL's requirements.** 2. **Minimum 500 Mbps of sustained SD-WAN throughput** with all features enabled, including DPI, NGFW, IPS/IDS, and TLS/SSL inspection, as defined in Section A and Section B.		
4	The site-level SD-WAN device must be sized with adequate CPU, memory, storage, and hardware acceleration to support local Internet breakout, multiple WAN links, per-application traffic steering, and integrated security functions (NGFW, IPS/IDS, URL filtering, TLS/SSL inspection) without any performance degradation. The Bidder shall be fully responsible for proper hardware sizing based on the required throughput under full feature load (including TLS/SSL inspection) and shall upgrade or replace the hardware at no additional cost if resource exhaustion impacts performance during the project period.		
5	**The SD-WAN site device must support integrated NGFW capabilities including, but not limited to:** • Zone-based firewalling • DoS/DDoS protection (application based) • Layer-7 / Application-based firewalling • URL filtering • Intrusion Prevention System (IPS) • Anti-malware/AV scanning • TLS/SSL inspection		

6	The SD-WAN site device must support Hub-and-Spoke, partial mesh (minimum 30 sites), and secure connectivity to DC, DR, HQ, and other designated sites as required. The device must reliably support the required number of overlay tunnels across all WAN links from Day 1. All necessary hardware and software resources must be provided to ensure high-performance multi-link tunnel formation across all supported topologies.		
7	SD-WAN site devices must support ingestion, storage, and enforcement of a minimum of 1,000 threat-intelligence IOC entries, including malicious IPs (IPv4/IPv6), domains, URLs, and FQDNs. Higher IOC capacity is preferred where supported by the OEM hardware. IOC policies may be delivered through the SD-WAN controller, middleware integrated with the WBSEDCL's Threat Intelligence (TI) platform, or by any OEM-supported method. The selected architecture must ensure that no additional latency, service degradation, or traffic disruption occurs during threat-intelligence processing. Any additional hardware, software, or performance optimisation required to achieve this shall be provided by the Bidder at no extra cost to the WBSEDCL.		
8	The SD-WAN site device must support integrated DHCP Server functionality for a minimum of 300 concurrent DHCP clients for A2 boxes and minimum 50 concurrent DHCP clients for A1 boxes, ensuring reliable IP address allocation, customized pool creation, even with all security features enabled. DHCP services must support large-scale lease management, binding tables, and required DHCP options without performance degradation.		
9	The SD-WAN site device must support NAT Traversal (NAT-T) or equivalent mechanisms to establish and maintain secure overlay tunnels (e.g., IPSec, GRE, VXLAN) when deployed behind NAT-performing routers, carrier-grade NAT (CGNAT), or firewalls. This ensures that local internet breakout and secure branch connectivity function seamlessly without requiring public IPs or perimeter reconfiguration.		
10	All SD-WAN site devices shall be installed in the WBSEDCL's 6U/9U rack enclosures. The OEM/System Integrator must supply all required rack-mount kits, brackets, shelves, and accessories to ensure secure, stable, and standards-compliant installation.		

<u>Section C.</u> High-End SD-WAN device Specifications (DC / DR / HQ)

Applicable Device Categories:

- **Type-B1** – 4 Nos.
- **Type-B2** – 2 Nos.
- **Type-B3** – 2 Nos.

1	All high-end SD-WAN devices must support every capability defined under **Section A (SD-WAN Device Technical & Functional Requirements)** to ensure secure, reliable, high-performance WAN connectivity.		
2	Port Requirements & Base Hardware Specifications <u>Type-B1-</u> • **Minimum 8× 1G RJ45** and **4×10G SFP+** ports, with all ports being software-configurable and able to be assigned as WAN, LAN, or DMZ interfaces as per WBSEDCL's requirements. • **Minimum 20 Gbps sustained throughput** with *all feature sets enabled*, including NGFW, IPS/IDS, VRF, as defined under this Section and Section A. <u>Type-B2 (Medium-Capacity DC/DR / Hub Appliance)</u> • **Minimum 10 × 1G RJ45** and **4×10G SFP+** ports, with all ports being software-configurable and able to be assigned as WAN, LAN, or DMZ interfaces as per WBSEDCL's requirements. • **Minimum 10 Gbps sustained throughput** with *all feature sets enabled*, including NGFW, IPS/IDS, **TLS/SSL inspection** as defined under this Section for this box type and Section A. • Device must support hardware acceleration for TLS inspection (SSL offload engines) to maintain performance at DC scale. <u>Type-B3 (Lower Capacity Hub / Regional Node Appliance)</u> • **Minimum 8× 1G RJ45** and **4×10G SFP+** ports, with all ports being software-configurable and able to be assigned as WAN, LAN, or DMZ interfaces as per WBSEDCL's requirements. • **Minimum 2 Gbps sustained throughput** with *all feature sets enabled*, including NGFW, IPS/IDS, **TLS/SSL inspection** as defined under this Section for this box type and Section A. • Device must support hardware acceleration for TLS inspection (SSL offload engines) to maintain performance at DC scale.		

	The **SFP+ transceivers** will be provided by the System Integrator (SI) as per project requirements and must be sourced from the **same OEM or an OEM-authorized manufacturer**.		
3	For type B1 - (where external and internal firewall present)- The device must support following basic NGFW security capabilities but not limited to, the following: • **Zone-Based Protection**: • **DoS/DDoS protection (application based)** • **Layer 7 Firewall and Application based Control**: • **URL Filtering** • **Intrusion Prevention System (IPS)** For type B2 and B3- The device must support **core Next-Generation Firewall (NGFW) features**, including but not limited to: • **Intrusion Prevention/Detection (IPS/IDS)** • **L7 firewall** • **Anti-malware protection** • **URL filtering** • **DoS/DDoS protection (application based)** • **VRF-based segmentation** • **NAT/PAT (Static and Dynamic)** • **TLS/SSL inspection**		
4	• Must support **virtualization** (minimum **10 virtual firewall instances**). • The device may be deployed as an internal or external firewall and must protect both internet-facing and east-west/internal traffic. • Must deliver DC-grade performance with *no perceptible latency* under full load.		
5	Devices must support BGP Route Reflector functionality and policy-based routing with asymmetric route handling.		
6	The device must support both Active-Active and Active-Passive operating modes, and must be configurable to run in either mode as per the network design. It must ensure seamless, sub-second failover between		

	active and standby paths or components, without session drops or service degradation		
7	The Device must have internal dual hot swappable power supply.		
8	The solution must support advanced WAN path conditioning techniques such as packet duplication and forward error correction (FEC), to ensure lossless delivery and seamless performance of real-time applications (e.g., voice, video, VDI) across unreliable or degraded WAN links.		
9	Device must support: • Multiple **VRFs** for WAN/LAN/DMZ segmentation • Creation of multiple **DMZ zones** • Strict north–south and east–west policy enforcement • Inter-VRF route-leaking with policy control		
10	The device must support a minimum of 200 concurrent Remote Access VPN users connecting from outside the WBSEDCL's network (over the Internet) using the OEM's **ZTNA-enabled VPN client.** The solution must enforce application-level access control (Zero Trust), identity- and posture-based session enforcement, and must use pooled/concurrent licensing across the deployment.200 concurrent remote access VPN users (OEM's ZTNA-enabled client). These remote users, connecting from outside the WBSEDCL's network over the Internet, must be able to securely access authorized enterprise applications hosted across all Type-B high-end SD-WAN locations (DC, DR, regional hubs). Multi-Factor Authentication (MFA) must be supported for ZTNA clients, access through integration with the WBSEDCL's SMS gateway for one-time passcodes. ZTNA VPN agent must support Windows 10 and onwards, macOS, Linux(RHEL/Ubuntu/Debian) with low CPU/memory footprint, background operation, and auto-update		
11	The device must be capable of forming and operating within Hub-and-Spoke, Partial Mesh, and Full Mesh topologies — connecting seamlessly with all site offices (up to 1000 locations**)** as per the network design and configuration. The device must reliably handle the required number of secure overlay tunnels across all sites having 4 WAN links each (MPLS/internet) from Day 1, with no performance degradation. It must be provisioned with sufficient hardware and software resources to ensure high-performance, multi-link tunnel formation under full load.		

12	Devices must include sufficient CPU, memory, storage, and acceleration modules to support: • High tunnel density • Full NGFW stack • TLS/SSL inspection (as per box type) • DC-class routing • Peak-load performance **Bidder shall upgrade/replace hardware at no additional cost** if resource shortfall impacts performance at any point during the project period.		
14	Devices must support NAT-T or equivalent mechanisms compatible with: • thousands of branch devices • mixed carrier-grade NAT environments • firewalls and load balancers in front of DC/DR boxes		

Annexure-T-3

Compliance Sheet: SD-WAN Controller / Manager / Orchestrator

Sl. No.	Specification	Compliance (Yes/No)	Remarks
1	Must be deployable as a Virtual Appliance or Software-based solution. All required components—including operating system, hardware specifications (if any), licenses, and associated software must be bundled and supplied as part of the on-premises solution.		
2	Must be provisioned with adequate compute resources (CPU, memory, storage) to ensure stable performance under full operational load. The solution must not exhibit performance degradation when managing all licensed SD-WAN devices and features concurrently.		
3	Must be licensed to manage all Hub and Branch SD-WAN CPE devices, with scalability to support at least 1000 edge devices.		
4	Must support HA deployment (Active-Active or Active-Passive) between DC and DR, with seamless failover and configuration synchronization. DC and DR shall be in different geographic locations.		
5	Must support Zero Touch Provisioning (ZTP) and template-based provisioning/configuration of SD-WAN CPEs from a centralized console.		
6	Must provide real-time and historical monitoring of each WAN link (latency, jitter, bandwidth, SLA) with graphical SLA violation reports and alerts.		
7	Must provide a geo-map visualization of all Hub and Spoke locations with real-time status overlays. The map should show link health using color-coded indicators (e.g., Green for all links up, Yellow for single link, Red for all links down) and allow drill-down to site/device status and alerts.		
8	Must support global policies and objects for SD-WAN devices — including NGFW features such as IPS, Domain/Hostname-based filtering, URL Filtering, Geo-IP blocking, which can be centrally created on the controller/manager and pushed to all or selected SDWAN devices. The system must allow object re-use across policies, support bulk updates, and maintain version control for rollback.		
9	The solution must support distribution and application of all patches and updates for all supported features and components from Day 1 of deployment, as released by the OEM, throughout the device lifecycle.		
10	The SD-WAN controller /solution must support ingestion and enforcement of IoCs (Indicators of Compromise)-domains, URLs, IPs. through its policy or access rules and apply them on site SDWAN boxes**.** STIX/TAXII (2.x support or latest industry standard) is preferred. The solution must also be capable of integrating with threat intelligence feeds in common formats such as CSV or JSON via APIs or external connectors or middleware solutions with Threat Intelligence Platforms. The controller/solution must provide central override/replace capability to update or withdraw rules or policies implemented for an IOC.		
11	Must support integration via RESTful APIs, scripts, or native connectors with NAC/AAA backed by integration with centralized directories (AD, LDAP, LDAPS), NMS, and SIEM platforms.		
12	Must support automatic configuration backup and revision tracking for every change in SDWAN devices. Admins should be able to view, compare, and roll back previous configuration versions. Export for archival must be supported.		

13	Configuration & Change Management: The SD-WAN controller must support template-based (or equivalent) configuration with group-level templates (e.g., branch, HQ, DR) and per-device overrides, ensuring consistency and scalability. It must allow automatic template application on onboarding/replacement, and **s**upport version control, rollback, bulk updates, and preferably role-based approval workflows for configuration changes		
14	Must allow defining configuration baselines and trigger alerts (on dashboard or email) upon deviations. An audit log must record timestamp, user ID, and configuration data.		
15	Must provide a secure, plugin-free Web UI based on modern technologies (HTML5/JS) and a Command-Line Interface (CLI) for advanced operations. Access control must include IP-based restrictions.		
16	Must support multi-user access with RBAC. At minimum, support: - 5 full-admin users (config/policy) - 10 read-only users (monitoring/audit) - Custom roles (e.g., SI support, Security Admin, Ops) Role permissions must be configurable per interface (Web UI/CLI).		
17	The controller/solution must maintain and display at least 180 days of historical monitoring data (e.g., link performance, traffic analytics, device health, alerts) within its dashboards, with capabilities for graphing, trend forecasting, and data export for reporting purposes.		
18	The controller must support NAT-T (NAT Traversal) mode and function without degradation when deployed behind a firewall and load balancer, or internal network segment.		
19	The SD-WAN controller must support certificate-based mutual authentication for all edge devices. Each device must present a unique X.509 certificate signed by a trusted CA (OEM or Enterprise based), with serial/device ID embedded. The controller/orchestrator shall validate both the certificate chain and serial/device ID during onboarding.		
20	The SD-WAN controller/solution must centrally create, modify, and deploy DHCP scopes, reservations, and DHCP security features (e.g., DHCP Snooping, IP Source Guard, rogue DHCP detection) to one or more SD-WAN devices through templates or policy-based deployment.		
21	The SD-WAN controller/solution must provide dashboard-based visibility of DHCP lease and reservation information for all managed SD-WAN devices, displayed on a per-site or per-device basis as supported by the OEM. The dashboard must show sdwan devices MAC-to-IP bindings, hostnames, lease expiry, reservation status, and search/filtering by site, device, or MAC/IP.		
22	The SD-WAN controller must centrally push, monitor, and report compliance of DNS policies—including DNS forwarding, split DNS, and Internet/Intranet breakout rules—across all managed SD-WAN devices.		
23	The SD-WAN controller must centrally create, deploy, and monitor TLS/SSL inspection policies—including inspect/bypass rules, certificate distribution, and policy consistency checks—across all managed SD-WAN devices as per WBSEDCL security policy.		

Annexure-T-4

Compliance Specification: 24-Port L2 Managed Switches

Sl. No.	Technical Requirement	Compliance (Yes/No)	Remarks
1	Hardware & Interfaces: The switch must provide24 × 10/100/1000 RJ-45 access ports, plus at least one dedicated RJ-45 uplink port (≥1G) for direct Ethernet connection to the SD-WAN box. One more additional uplink port (RJ-45 or SFP) shall be provided for expansion Where SFP uplinks are used, the OEM/System Integrator must supply all required SFP transceivers including RJ-45 SFP modules (copper SFPs) if needed.		
2	Layer-2 features – IEEE 802.1Q VLAN (≥ 256), VLAN trunking, dynamic VLAN assignment via NAC (802.1X).		
3	The switch must support NAC-driven authorization with IEEE 802.1XandMAC-based authentication (MAB)**,** RADIUS VLAN assignment per RFC 3580 (Tunnel-Type/Medium-Type/Private-Group-ID**),** RADIUS Change of Authorization per RFC 5176**,** guest/unauthorized (fail-open) VLAN fallback**,** and RADIUS-provisioned per-session policy/ACL(e.g.,Filter-Id or equivalent).		
4	Security filtering – DHCP Snooping, IP Source Guard, Dynamic ARP Inspection, Storm-control, Port Security (MAC locking / aging).		
5	QoS & Multicast - QoS and multicast features including multiple queues per port (≥ 4), DSCP/CoS mapping, rate-limit and priority queuing; IGMP v2/v3 snooping and MLD snooping for CCTV multicast.		
6	Port mirroring (SPAN/RSPAN or equivalent); loop-guard or equivalent; broadcast/unknown-unicast suppression; cable diagnostics.		
7	Telemetry & Mgmt-SNMPv3, Syslog, RMON, and flow telemetry (sFlow/IPFIX/NetFlow-equivalent); SSH CLI & HTTPS GUI; IPv4/IPv6 management.		
8	The L2 managed switch may **preferably** support REST/NETCONF/OpenConfig APIs for SDN/IPAM integration. This is desirable and not mandatory		
9	24-port managed switches shall be deployed in the WBSEDCL's 6U/9U rack enclosures**.** The OEM/System Integrator must supply all required rack-mount kits, rails, or accessories to ensure secure installation**.**		
10	Role-based admin accounts. Password policy enforcement.		
11	For NAC / EDR posture enforcement, the switch must support RADIUS Change of Authorization (RFC 5176) to quarantine ports on NAC trigger.		
12	LLDP/LLDP-MED for endpoint discovery.		
13	Capability to integrate with SIEM solution and log server		
14	Support STP (802.1D), RSTP (802.1w), MSTP (802.1s) with per-VLAN configuration, BPDU,Root,Loop Guard, PortFast (or equivalent), and port mirroring (SPAN/RSPAN or equivalent). Must interoperate with other vendors for loop prevention.		
15	The switch must provide non-blocking switching fabric capacity to support full line-rate, full-duplex traffic on all ports simultaneously (e.g., ≥ 48 Gbps for a 24 × 1 GbE model, or higher for models with additional 10 GbE uplinks)		
16	The switch must support configurable management session timeouts and maintain detailed logs of all configuration changes, including the user ID, timestamp, and description of each change, to ensure security and ISO 27001 compliance.		
17	The switch must support configuration backup and restore functionality to enable rapid recovery and ensure operational continuity in case of hardware failure or misconfiguration.		

18	All managed L2 switches must support assignment of a management IP (IPv4/IPv6) in a dedicated management VLAN **t**o enable centralized discovery, configuration, and monitoring by the switch controller. This does not require routing capability on the switch; the management interface is solely for controller communication. For cascaded/extended site switches, the controller must be able to manage them individually via their management IP, even when connected behind another access switch.		
19	The switch must support cascaded/extended deployment, where additional switches can be connected behind a site switch via uplink or trunk ports, with full forwarding of all configured VLANs and NAC/AAA policies. The controller must manage cascaded switches individually through their management IPs.		

Annexure-T-5

Centralized Switch-Controller – Technical & Functional Requirements

Sl. No.	Technical Requirement (Controller / NMS)	Compliance (Yes/No)	Remarks
1	Manage at least **1,000** 24-port L2 switches.		
2	The controller/solution must support deployment in DC and DR with automated configuration backup and synchronization and seamless switchover to the DR instance in case of DC failure.		
3	Unified dashboard – Auto-discover switches, show topology, port status, PoE budget (optional), traffic graphs, switch asset list with MAC id etc.		
4	**Configuration & Change Management:** The controller must centrally store switch configuration templates and support flexible template-assignment mechanisms suitable to the OEM's architecture. It shall apply the appropriate template during device onboarding or replacement and support re-provisioning of replacement switches using stored templates/configurations. The system shall support version control, roll back, bulk updates, and preferably role-based approval workflows for configuration changes.		
5	The solution shall support granular role-based access control, including separate roles for view-only, configuration, and audit functions, with centralized authentication and authorization through NAC-AAA backed by integration with AD/secure LDAP. The solution shall also support 2FA for administrative users, with email (SMTP-based) or SMS-based OTP as the second factor.		
6	Security Monitoring – Alert on DHCP Snooping violations, MAC flap, port-security hits; forward events to SIEM in CEF/Syslog.		
7	Capability to integrate with the SIEM solution and log server		
8	The centralized Switch Controller shall maintain a built-in audit trail recording all administrator actions, including user ID, timestamp, and a detailed description of each action. The solution shall also support forwarding these audit logs to the Log Server supplied under this project for centralized storage, correlation, and retention.		
9	The centralized switch controller must support secure adoption and management of all site switches over routed IP/SD-WAN paths, including switches cascaded behind other site switches. Adoption must be possible via pre-provisioning, join tokens, DHCP/DNS discovery, or equivalent.		
10	The controller shall support automated backup and restore of switch configurations, controller settings, templates, and policies, including scheduled backups and secure storage of backup files.		
11	The controller shall provide open APIs (such as RESTful or equivalent APIs) to integrate with third-party systems for monitoring, automation, orchestration, ITSM/ticketing tools, or other management workflows.		
12	The controller shall provide health monitoring for L2 switches, including CPU, memory, temperature, port status, interface errors, and traffic statistics.		

Annexure-T-6

Specification for Indoor Access point (Wi-Fi)			
Sl. No.	**Description/Features**	**Compliance Yes/No**	**Remarks**
1	The Access Point should support Wi-Fi 6 standard.		
2	Must have the Tri-radio option to support Radio1 as 2.4 GHz and Radio2 as 5 GHz devices and Radio 3 as 2.4GHz/5 GHz for frequency scanning.		
3	Should have Minimum 1x100/1000/2500 Base-T RJ45, 1x10/100/1000 Base-T RJ45		
4	Maximum power consumption should not be more than 30 W.		
5	Should support 4x4 MIMO		
6	The access Point should support throughput in Radio 1: up to 276 Mbps, Radio 2: up to 1200 Mbps, Radio 3: Up to 2401 Mbps.		
7	Should support Peak antenna gain of minimum 4 dBi in 2.4 GHz and 5 dBi in 5 GHz band		
8	Access point should support SSID's in Tunnel, Bridge, Split-Tunnel and mesh mode.		
9	Should support 16 at least Simultaneous SSIDs		
10	Should support following EAP types : EAP-TLS, EAP-TTLS, EAP-SIM, EAP-AKA		
11	Access point should support IEEE standards 802.11a, 802.11b, 802.11d, 802.11e, 802.11g, 802.11h, 802.11i, 802.11j, 802.11k, 802.11n, 802.11r, 802.11v, 802.11w, 802.11ac, 802.11ax, 802.1Q,802.1X, 802.3af, 802.3at		
12	Should have physical security lock (such as Kensington lock)		
13	The access point must support both ceiling and wall mounting, and all required mounting accessories shall be included in the box; if not, the bidder must quote all necessary mounting kits.		
14	Access point should support below Wireless Monitoring Capabilities a) Rogue Scan Radio Modes should support both background and dedicated modes. b) WIPS / WIDS Radio Modes should support both background and dedicated. c) Should support Spectrum Analyzer.		
15	Must support Reliable Video streaming to maintain video quality		
16	Must support QoS and Call Admission Control capabilities.		
17	Access Point should have built in NAC functionality to allow secure onboarding of devices		
18	The proposed wireless solution support client load balance features like		

	a) Access Point Hand-off -If the load on an access point (ap1) exceeds a threshold then the client with the weakest signal will be signaled by wireless controller to drop off and join another nearby access point (ap2)		
	b) Frequency Hand-off - the wireless controller monitors the usage of 2.4GHz and 5GHz bands, and signals clients to switch to the lesser-used frequency automatically		
19	Access point should independently scans the most available channels that do not interfere with other APs. It should support full time scan and periodically performs scan in the background scan for every ten minutes or can be adjusted. Channel change log should be recorded at controller.		
20	Rogue AP detection and mitigation should work on background and full-time scan to actively prevent valid users from connecting to Rogue AP.		
21	Wireless Solution should provide a wide range of information pertaining to the associated wireless clients to the administrator in a simple GUI.		
	a) Access Point and SSID Associated.		
	b) Association Time.		
	c) User ID Information and Device Type.		
	d) IP Address Assigned and MAC-Address Used.		
	e) Channel and Bandwidth Used.		
	f) Currently Signal Strength,		
	g) 802.11 Technology Type and MIMO used		
22	Solution must provide detailed view of all Applications traffic traversing the Access Point originating and destining for each specific wireless station		
23	The access point must support wireless mesh to eliminate the need for Ethernet wiring by connecting WiFi access points to the controller by radio.		
24	Access Point must have two nos. Ethernet port that operates as a WAN port to provide management connection to a WiFi Controller and another LAN to provide a wired network access and should also be soft configurable and act as redundant port if required.		
25	Wireless Controller should have facilities like spectrum analysis, rouge AP detection and suppression, per radio and per SSID users load, bandwidth utilization etc.		
26	Access point should be controller based.		
27	Access point Operating Temperature should be: 0 - 45°C		
28	Access points must have logging feature to maintain trail		
29	The wireless solution must interoperate seamlessly with the centralized NAC/AAA platform and, where applicable, with the SD-WAN/NGFW, ensuring coordinated enforcement of CoA actions, dynamic VLAN assignment, role-based access, posture checks, and per-user/application visibility. This is required to maintain uniform authentication, security, and compliance across wired and wireless networks.		

Annexure-T-7

Wireless Controller Specification			
S.No.	**Specification**	**Compliance Yes/No**	**Remarks**
1	On-premise controller (does not require cloud for management)		
2	Supports up to 100 Access Points (APs)		
3	Supports up to 1,000 simultaneous clients		
4	Supports Wi-Fi standards: 802.11a/b/g/n/ac/ax		
5	Supports 2.4 GHz, 5 GHz, and 6 GHz bands (Wi-Fi 6E)		
6	Supports MIMO (e.g., 2x2 MIMO, 4x4 MIMO)		
7	Maximum throughput supported: e.g., 2 Gbps, 4 Gbps		
8	Includes wired Ethernet ports (e.g., 2x 2.5 Gbps, or SFP for fiber)		
9	Supports redundancy and failover (N+1, N+N, active/passive, active/active)		
10	Security features: WPA2/WPA3, 802.1X, MAC filtering, captive portal, RADIUS, VPN support		
11	Guest network support with captive portal, VLANs, and QoS for guest traffic		
12	Quality of Service (QoS): traffic prioritization, rate limiting, app-aware QoS		
13	Load balancing across APs and client session distribution		
14	Supports multicast: IGMP snooping, multicast-to-unicast conversion, or equivalent.		
15	Wireless mesh networking support between APs		
16	Real-time monitoring, analytics, heatmaps, SSID/client reports		
17	Certifications and compliance: CE, FCC, UL, Wi-Fi Alliance, HIPAA, PCI DSS		
18	Management via web GUI, CLI, or mobile app		
19	API support: RESTful API, SNMP, Syslog integration		
20	Scalable to 100 APs with multi-site, centralized management		
21	Supports single-site and multi-site deployments with remote AP management		
22	Detailed client visibility: device type, OS, posture, NAC integration		
23	Supports firmware/software updates, with rollback and version control		
24	There must be adequate settings available in the controller console to disable remote management, SSID broadcast, and other administrative functions of Wi-Fi access points, as required.		

Annexure-T-8

NAC, AAA and related solutions requirements-

The proposed solution for Network Access Control (NAC), Authentication, Authorization, and Accounting (AAA), Captive Portal, and Internet Traffic Control shall be deliverable either through a single integrated platform or via multiple dedicated devices/modules, provided full compliance with the functional, security, and performance requirements listed in the respective sections. All components must be on-premises, support high availability across DC,DR, and integrate seamlessly with the SD-WAN, managed switches. NAC-AAA agent needs be installed at endpoints.

A. NAC Feature Compliance Checklist

Sl. No.	NAC Feature Requirement	Compliance (Yes/No)	Remarks
1	Endpoints must pass posture checks for OS type, version, patch status, EDR presence; devices without NAC agent or with non-compliant posture must be denied internet access and placed in a restricted VLAN with only local intranet access/no access as per requirement		
2	Compliant endpoints must be assigned to the Production VLAN with full access as per policy. Non-compliant or posture-failed endpoints must be assigned to Restricted/Quarantine VLANs using RADIUS CoA or equivalent mechanisms.		
3	The Restricted/Quarantine VLAN must be configurable to allow limited network or intranet access to designated servers (e.g., DC/critical application servers) if required, ensuring essential business services are not disrupted in case of NAC agent absence or posture-check failure. This capability must be supported without compromising the enforcement of internet access restrictions.		
4	NAC agent must support Windows 10 and onwards, macOS, Linux (RHEL/Ubuntu/Debian), with low CPU/memory footprint, background operation, and auto-update.		
5	PCs where the agent cannot be installed must be blocked from internet/intranet or placed in restricted VLANs as per policy.		
6	Remote agent deployment via scripts, GPO, or equivalent automation must be supported.		
7	Agentless profiling for non-PC devices (printers, CCTV, biometric, IoT, VC systems) via MAC, SNMP, DHCP, with device-specific VLANs.		
8	Unauthorized device movement or IP changes must trigger alerts.		
9	Real-time posture compliance and authentication dashboards.		
10	Exportable compliance reports (CSV/PDF) for posture compliance and authentication.		
11	Must support API integration with EDR solutions for agent status and posture validation.		
12	From Day-1, the NAC platform must support **10,000 PCs** (agent-based), **10,000 headless devices** (agentless profiling via MAC/SNMP/DHCP), and all project servers/controllers/devices/log servers, with full posture checks, VLAN assignment, and policy enforcement as per specification.		
13	The NAC solution must support posture assessment for at **least 200 concurrent remote ZTNA clients** connecting over the Internet, ensuring compliance with defined security policies (OS patch status, AV/EDR presence, etc.) prior to granting access.		

14	High-availability clustering across DC and DR, with SD-WAN integration for propagating access control decisions.		
15	Licensing for the NAC solution shall not be restricted or limited based on features, device templates, number of ports, concurrent sessions, throughput, or any similar parameter. The bidder must provide all functionalities requested in the Technical Annexure		

B. AAA Feature Compliance Checklist

Sl. No.	AAA Feature Requirement	Compliance (Yes/No)	Remarks
1	Must support RADIUS and TACACS+ for authentication, authorization, and accounting.		
2	Integration with LDAP,LDAPS,AD for user authentication and role assignment.		
3	Role-based access control (RBAC) with VLAN, ACL, and QoS policy mapping.		
4	Detailed accounting logs for all user sessions (start/stop time, device MAC/IP, VLAN).		
5	Support for per-user and per-device policy mapping, including multiple device associations.		
6	High availability with full state synchronization between DC and DR nodes.		
7	Export of AAA logs to SIEM in real time; Also retention of logs as per CERT-In/ISO 27001:2022 or latest (at least 180 days).		
8	Administrative access to AAA platform must be role-segregated with MFA support.		
9	Support CoA (Change of Authorization) and session re-auth based on policy triggers (e.g., posture failure).		
10	API access for integration with orchestration, ticketing, and monitoring systems.		
11	Must integrate and work smoothly with managed switches, SD-WAN, and all other solutions in this project.		
12	From Day-1, the AAA platform along with the devices in coordination must support at least: • **10,000 PC users** (agent-based NAC), • **800 SD-WAN devices** (~8 authenticated users per device: 2 SI engineers, 4 WAN-vendor NOC users, 2 WBSEDCL users), • **850 managed switches** and **12 Wi-Fi access points** (~4 authenticated users per switch and ~4 per Wi-Fi AP), • **200 ZTNA VPN users**, and • **servers, controllers assigned in this project** (~6 authenticated users for 20 server/controllers).		

C. Captive Portal & Internet Traffic Control Compliance Checklist

The captive portal shall be implemented as a unified internet access control mechanism for **all enterprise users**, including those connected via **LAN or Wi-Fi**, ensuring that every user authenticates through **LDAP,LDAPS,AD** in coordination with **NAC/AAA** before internet access is granted. The portal shall enforce posture and compliance checks uniformly across both wired and wireless networks.

Sl. No.	Feature Requirement	Compliance (Yes/No)	Remarks
1	Captive portal must authenticate users via LDAP,LDAPS,AD in coordination with NAC/AAA and integrate posture checks for compliance before providing access.		
2	The captive portal shall support configurable user session and idle timeout values, allowing administrators to define and modify default durations (e.g., 8–12 hours of session validity and 30–60 minutes idle timeout).		
3	The system shall prevent unintended user logout by maintaining session persistence during network reconnections and ensure re-authentication only occurs as per defined security policy.		
4	User identity must be linked to device for policy enforcement; logs must capture user-device association.		
5	The captive portal shall support self-registration workflows for **Guest and BYOD users**, allowing them to request temporary access to the network through a secure onboarding interface. The solution must support **automatic time-bound account creation**, where guest or BYOD access credentials expire automatically after a configurable duration (e.g., 8 hours, 24 hours, or 7 days).		
6	Guest/BYOD workflows with sponsor approval, time-bound accounts, and AUP acceptance must be supported.		
7	The captive portal shall enforce **Acceptable Use Policy (AUP)** acceptance by displaying WBSEDCL defined terms and requiring user consent before granting network access.		
8	The system shall support **sponsor or designated approver validation**, whereby an authorized employee receives and approves guest access requests via portal, email, or notification before access is granted.		
9	Captive portal must support full customization (logo, branding, messages, disclaimers, or instructions) to display WBSEDCL -specific information to users during authentication/guest onboarding, either natively or via NAC/AAA integration and or via scripts .		
10	From Day-1, the captive portal must support authentication and posture checks for at least 10,000 PC/laptop users, along with guest/BYOD and VPN/ZTNA users, as per NAC/AAA integration requirements, without impacting authentication or policy enforcement performance.		

11	The captive portal must be scalable to handle the full 5-year projected load in line with NAC and AAA licenses and user support , with hardware ,related software and architecture sized that no performance degradation occurs . Additional licenses for expansion shall be procured as required.		

D**. Identity-Integrated Internet Access Control Compliance Checklist-**

This checklist defines the compliance framework for **Identity-Integrated Internet Access Control implemented for wired and wireless users**, which serves as the primary internet breakout and enforcement point. It ensures secure and policy-based management of internet usage for approximately **10,000 users**. A separate dedicated device **may or may not be required**, provided the required functionality is achieved using components within this project — including **NAC, managed switches, Wi-Fi,SD-WAN controllers, log servers, and reporting tools** — along with the WBSEDCL 's existing directory services (**LDAP,LDAPS,AD**). The framework ensures that all user traffic is **authenticated, monitored, and controlled** in accordance with the WBSEDCL 's security, compliance, and usage policies.

Sl. No.	Feature Requirement	Compliance (Yes/No)	Remarks
1	Must log all internet restriction events due to non-compliance.		
2	Internet access control must support per-user/group policies (via LDAP,LDAPS,AD, in coordination with NAC/AAA identity mapping).		
3	Support time-based and quota-based internet access restrictions at user and group levels. The solution shall allow administrators to define time-bound permissions — for example, permitting access to high-bandwidth or video-streaming sites for specific periods or designated user groups — in accordance with WBSEDCL policies.		
4	URL categorization & filtering with custom category creation; block high-risk categories.		
5	Allow/block lists shall be configurable at branch, user, and group levels. The solution must support granular, identity-based policy creation — for example, permitting access to coding and development related websites for the "Developer" group while restricting such access for other user groups — in alignment with WBSEDCL internet usage policies.		
6	Application-level visibility and control for key platforms (e.g., YouTube, torrents).		
7	Scheduled/on-demand internet usage reports by user/group/branch/category; exportable in CSV/PDF.		

8	Integration with NAC for posture-based internet policy enforcement.		
9	The internet access control solution shall integrate with SD-WAN and routing components to ensure user/group traffic follows WBSEDCL policies for local breakout or centralized inspection.		
10	Must support real-time visibility and analytics of internet usage by user ID, device, branch, and application for proactive monitoring and optimization.		

Annexure-T-9

Reports, Dashboards & Analytics Compliance Sheet

This annexure defines the reporting, dashboard, and analytics compliance requirements for the proposed solution. The objective is to ensure that all deployed components — including SD-WAN, Managed Switches, NAC, AAA, and IP Address Management — provide centralized, consistent, and audit-ready reporting capabilities.

The reporting framework must deliver both real-time dashboards for operational visibility and historical data retention for compliance and audit purposes. These requirements may be fulfilled either through an integrated (in-built) reporting and dashboard system or through a reporting platform aggregating data from all components or if any additional accessories for generation of the reports if required (in case the supplied system doesn't have the same capabilities).

General Reporting Compliance – Applicable to All Reports Dashboards and Reporting Systems in this project.

Sl. No	Requirements	Compliance (Yes/No)	Remarks
1	The reporting must include real-time (live dashboards) with role-based Access support and historical data across all devices and solution components, with a minimum retention of 180 days.		
2	For SLA parameters such as WAN link availability, device availability, and downtime (in minutes), the system must provide consolidated monthly reports and retain this data for at least two (2) years (where applicable)		
3	Reports containing user or application data must support masking/anonymization of sensitive fields to meet privacy and compliance requirements.		
4	The reporting system must support integration with external platforms through standard APIs.		
5	All reports, including configuration change reports, must include user ID, timestamp, and be tamper-evident, ensuring a complete audit trail.		
6	The reporting system must generate monthly compliance reports and support real-time alerts for performance issues, threshold breaches, and security incidents.		
7	The reporting system must provide automatic emailing for scheduled reports periodically to configured email addresses		
8	The reporting system must allow users to download/export reports in PDF, HTML, and an editable Excel-compatible format (such as CSV or equivalent).		

A. SDWAN related Reports, Dashboards & Analytics Compliance Sheet-

Sl. No	Requirements	Compliance (Yes/No)	Remarks
1	Support concurrent analytics from up to 1000 SD-WAN CPE devices.		
2	Centralized analytics platform can be Physical, Virtual, or Software-based, with OS and hardware bundled.		
3	Role-Based Access Control (RBAC) with secure LDAP/Active Directory integration, allowing alignment with NAC and AAA systems.		
4	Customizable user roles and permissions, including tailored dashboards for up to 100 designated 'regional heads' overseeing multiple sub-sites.		
5	Customizable interactive dashboards and summary views.		
6	Drill-down capabilities to trace user sessions, bandwidth consumptions, application flows, and transactions.		
7	Advanced visualization including charts and geolocation-based maps, showing the status of sites on the map of West Bengal.		
8	NOC view for centralized monitoring with multi-site status overview dashboards.		
9	Visibility and asset inventory of all SD-WAN components across DC/DR, including IP, Software version, MAC, location, and device type.		
10	Enhanced analytics for bandwidth, SLA metrics (latency, jitter, MOS), application usage, and security threats.		
11	Per-path application SLA reporting with latency, jitter, packet loss, and MOS/equivalent scores.		
12	Real-time and historical monitoring of DIA vs MPLS utilization, including percentage split and trend reports, including Local Internet Breakout (LBO) traffic visibility with application categories, usage, and risk levels.		
13	Top applications consumption and Top talkers users by bandwidth utilization, with graphical representation per application/user.		
14	QoS/CoS bandwidth utilization monitoring and class-based reporting.		
15	Live tunnel view for application policy transport usage and provide overall health summary dashboards showing number/percentage of active, degraded, or down tunnels per transport type.		
16	Policy hit/miss reporting to measure SD-WAN forwarding policy effectiveness.		
17	Reports and live dashboards for sites with single link, no link, or multiple links.		

18	Daily, weekly, monthly downtime reports in minutes for all WAN links and devices. Location-wise and IP-wise site availability dashboards and reports summarizing uptime %, SLA compliance.		
19	Reports related to SD-WAN controller health, control-plane latency, overlay establishment success/failure.		
20	The system must display DHCP-related statistics and reports from all SD-WAN devices, including assigned IP addresses, available/free IPs in each pool, MAC-to-IP bindings, lease expiry details, and DHCP allocation trends. Reports shall be system-generated and available per site and per subnet, with an option to compile a consolidated summary report either automatically or manually as required.		
	Network Security Reporting		
21	The SD-WAN solution must include traffic anomaly detection and reporting capabilities, providing visibility into network health and performance across all WAN transport types (MPLS, DIA, Broadband, etc.). The solution must be able to generate reports/alarms on suspicious traffic patterns, such as unexpected application behaviors, bandwidth anomalies, and traffic bottlenecks, to assist with threat localization.		
22	The SD-WAN solution must include the ability to generate performance reports with network behavior analysis based on transport types (e.g., MPLS, DIA), highlighting potential risks, traffic abnormalities, and potential application issues. This analysis must be used for proactive network optimization and incident response coordination.		
23	The system must generate monthly security compliance reports covering suspicious traffic, transport-specific threat localization (e.g., MPLS, DIA), and policy hit/miss data. It must also deliver real-time alerts for performance issues, threshold breaches, and detected threats, including IPS/IDS events, NGFW hits, and other correlated security incidents.		
24	Provide dashboards and reports for TLS/SSL inspection showing total, decrypted, bypassed, and failed sessions, TLS versions/ciphers, and resource utilization impact, with options for on-demand or scheduled export.		
25	Provide centralized visibility and alerts for certificate validity, expiry, mismatch, and trust status across all devices, with exportable and email-based reports.		
	System & Alerts / Audit / Integration		
26	Forward logs to SIEM/SOC platforms or Log Server via Syslog, CEF, or API.		
27	Customizable report templates for investigation and incident response.		
28	Custom report creation with an intuitive chart and table builder.		

29	On-demand and scheduled reports in CSV, HTML, and PDF formats. System shall support automated periodic emailing of reports to configured recipients.		
30	The solution must provide automated alert notifications for performance issues, security incidents, and threshold breaches, including events such as link flaps at remote branch locations, ISP link quality degradation, WAN link utilization threshold breaches, and branch device health parameters (CPU, memory, and disk utilization).		
31	Integration with NTP,SNMP, Syslog, and REST API for alert and report automation and log time stamp management.		
32	Centralized dashboards or reports displaying configuration and policy change history across all SD-WAN controllers and edge devices.		
33	SD-WAN dashboards must support high-resolution NOC video-wall displays (45", 55", 65" or larger) and NOC-friendly multi-screen (VDA-style) views for continuous monitoring, whenever required, without any loss of resolution or real-time updates.		

B. Managed Switch Related Reports, Dashboards & Analytics Compliance Sheet-

Sl. No	Requirements	Compliance (Yes/No)	Remarks
1	Port status changes (up/down), speed, duplex.		
2	Spanning Tree Protocol topology changes and loop prevention alerts.		
3	VLAN membership and trunk status changes.		
4	Interface utilization (real-time & historical).		
5	MAC address table changes (learned, aged out, moved).		
6	Security events such as BPDU Guard, Port Security violations, unauthorized device attempts.		
7	Firmware and configuration change reports with user and timestamp.		
8	Error counters (CRC errors, alignment errors, packet drops).		
9	Inventory of switches with model, serial, location, and firmware version.		
10	The reporting solution for managed switches must provide **customizable dashboards** for switch health, interface utilization, VLAN and security status, and error monitoring.		
11	Reports related to Switch controller health, overlay establishment success/failure.		

12	The reporting solution must provide **monthly compliance reports** summarizing switch port security violations, unauthorized device connection attempts, Spanning Tree Protocol (STP) topology changes, and configuration change history, to support audit, security monitoring, and regulatory compliance.		
13	Managed switch dashboards must support high-resolution NOC video-wall displays (45", 55", 65" or larger) and NOC-friendly multi-screen (VDA-style) views for continuous monitoring, whenever required, without any loss of resolution or real-time updates.		

C. NAC Related Reports, Dashboards & Analytics Compliance Sheet-

Sl. No	Requirements	Compliance (Yes/No)	Remarks
1	Reports related to user authentication logs including 802.1X, MAC Authentication Bypass, and guest portal.		
2	Device posture assessment results reports with compliance/non-compliance status.		
3	Reports on Rogue device detection events.		
4	Report on failed authentication attempts categorized by reason (due to credentials, policy, posture etc.)		
5	Endpoint profiling reports including device type, OS, and location.		
6	VLAN assignment and policy application logs per authenticated session.		
7	Reports related to NAC policy hit/miss analytics.		
8	Real-time dashboard of authenticated vs unauthenticated device counts.		
9	Historical trends of device onboarding success/failures.		
10	The solution shall provide monthly compliance or equivalent reports summarizing authentication results, posture compliance, rogue device detections, and success/failure details for key NAC scans.		
11	Session Summary and User Correlation Dashboard-Provide dashboards and reports correlating users, devices, IP, MAC address, switch port, and authentication method (wired/wireless) for each active session, with search and filter options for troubleshooting.		
12	Integration Summary Reporting-Provide reports summarizing integration events with external systems (e.g., AD/secure LDAP, SDWAN, or SIEM), including synchronization status and last update time.		

D. AAA (Authentication, Authorization, and Accounting) Services Related Reports & Analytics Compliance Sheet-

Sl. No	Requirements	Compliance (Yes/No)	Remarks
1	Authentication related reports/logs for network device administration (CLI, GUI, API).		
2	Authorization policy application reports with user role mapping.		
3	Accounting records showing login/logout, command execution history, and session durations.		
4	ZTNA,VPN and remote access authentication reports/logs.		
5	Report on users created and deleted for at least last 180 days.		
6	Failed AAA requests categorized by cause (invalid credentials, role mismatch, policy violation).		
7	Must provide report of all privileged administrative access within its scope and be capable of exporting such reports for centralized audit.		
8	Reporting on concurrent user sessions and license usage.		
9	The reporting solution must provide comprehensive accounting records, including user login and logout times, command execution history, and session duration, to ensure full traceability of administrative and user activities.		
10	The reporting solution must generate monthly compliance reports summarizing failed authentication attempts (categorized by cause), privileged administrative access events, user account creation/deletion activities, and VPN/remote access usage trends, to support continuous monitoring and security audits.		
11	Provide real-time dashboards showing AAA system health, including RADIUS,TACACS+ request rate, authentication success/failure trends, and server resource utilization (CPU, memory, queue depth).		
12	Provide dashboards displaying active user sessions, authenticated devices, privilege levels, and session durations, with search and filter options by username, device, or IP address.		
13	Provide graphical dashboards summarizing authentication success/failure trends, top authenticated users, failed attempts by reason, and administrative access distribution across devices or regions.		

E. IP Address related Reporting Requirements Compliance Sheet-

May be provided through different systems such as SD-WAN controller, Switch controller, Wi-Fi controller, NAC/AAA, reporting/analytics platforms, or equivalent solutions)

Sl. No	Requirements	Compliance (Yes/No)	Remarks
1	Must provide an IP address–wise consolidated inventory of all active devices in this project—primarily covering all SD-WAN devices, all LAN switches, all servers/controllers, all Wi-Fi endpoints, and NAC/AAA-authenticated devices—through one or more centralized controllers, dashboards, or reporting solutions.		
2	Must be able to generate reports containing IP address, corresponding MAC address, device type, and hostname or authenticated user (as applicable for SD-WAN devices, switches, Wi-Fi APs, and NAC/AAA-authenticated endpoints).		
3	Site-wise IP address availability reporting for IP subnets configured under the SD-WAN solution, indicating used and available IP addresses at each site, through the SD-WAN controller, report analytics, or any equivalent mechanism.		
4	The system must support historical search and reporting of IP address usage, assignment, deletion etc. either within the platform's native retention capacity or through log server.		
5	Search and filter by IP, MAC, hostname or subnet across all managed devices in this project.		
6	Export IP address inventory and usage data in CSV, JSON, or API format for integration with external reporting or SIEM systems.		

F. Wi-Fi related Reporting Requirements Compliance Sheet-

Sl. No.	**Description/Features**	Compliance (Yes/No)	Remarks
1	Client Connectivity & Roaming Reports: Includes client session data, roaming events, client health, band selection, and NGFW integration for traffic/protocol-level insights.		
2	Access Point Performance: Reports AP status, channel utilization, signal strength, AP load, and RSSI.		

3	Network Utilization: Covers overall traffic load, data rates (avg/min/max), packet loss, and latency metrics.		
4	Interference & Noise Reports: Includes channel interference, co-/adjacent-channel interference, and noise floor readings.		
5	Coverage & Heatmap Analysis: Provides heatmaps for coverage, SNR, and capacity; helps in identifying signal gaps and AP planning.		
6	Error & Failure Analytics: Tracks authentication failures, DHCP issues, client disconnections, and roaming failures.		
7	Security & Policy Compliance: Reports on WPA2/WPA3 usage, policy violations, and captive portal access.		
8	Bandwidth & Throughput: Monitors per-client and per-SSID bandwidth utilization and throughput, with data rate insights.		
9	Health & Diagnostics: Includes AP availability, hardware (CPU, temperature, memory) monitoring, event logs, and RF health.		
10	Firmware & Software Management: Reports on version control, firmware/software update history, rollback capability.		
11	Application-Level Monitoring: Application analytics, traffic analysis per app, VoIP/video quality, app bandwidth usage.		
12	WiFi Attack Detection: Detects rogue APs/clients, evil twins, MAC spoofing, deauth attacks/suspicious wireless activity, DoS, packet injection, and AP impersonation.		
13	Configuration & Audit Compliance: Verifies SSID, encryption, VLANs, ACLs, DHCP, client isolation, firmware consistency, backup, logging, time sync, credential security, log retention, and admin activity tracking.		

Annexure-T-10

Log Server Solution Requirements & Log Types Compliance Sheet

The Log Server solution must integrate seamlessly with SIEM and other reporting platforms as per project requirements.

The log server must collect and retain logs from all devices and platforms included in this project, including but not limited to SD-WAN edge boxes, controllers, managed switches, NAC/AAA servers, captive portal, VPN gateways, and Internet access control/firewall components, ensuring centralized visibility and compliance.

The log server must retain logs as per CERT-In and ISO/IEC 27001:2022 (or latest) guidelines, ensuring compliance on log types and retention duration, while supporting security, compliance, and SLA monitoring requirements.

A. Log Server Requirements Compliance Sheet-

Sl. No	Requirements	Compliance (Yes/No)	Remarks
1	The solution must support log forwarding to third-party SIEM platforms using Syslog (UDP/TCP with optional TLS) and REST APIs carrying CEF/JSON log formats, ensuring complete fidelity of log data so the SOC SIEM can process logs seamlessly.		
2	Provide frequency control, rate limiting, batching, and retry logic for API-based log forwarding to ensure reliable delivery.		
3	Enable simultaneous log forwarding to SIEM and analytics/reporting systems without disruption. Must be able to operate in Active-Active or Active-Passive mode with one in DC and the other in DR for high availability and disaster recovery.		
4	Store all logs in structured, timestamped format for at least 180 days, in compliance with CERT-In/MeitY.		
5	Retain service-level parameter logs (each WAN-link, LAN-link, internet broadband downtime in minutes, SD-WAN device availability, switches availability, controllers availability) for 2 years hot storage for SLA analytics.		
6	Support customizable log parsing, filtering, and tagging for enrichment before forwarding.		
7	Maintain audit trails and real-time alerting for log delivery failures or SIEM endpoint issues.		
8	Support secure archival export via SFTP/FTP for long-term storage with tamper-evident controls.		

9	The solution must support dual-ingestion for log forwarding to multiple destinations in parallel and must also be capable of collecting logs on multiple ports simultaneously.		
10	The Log Server solution shall support **report generation (PDF, CSV, etc.)** for audit and analysis while ensuring that: • **Original log timestamps remain immutable and tamper-proof.** • Reports do not alter or overwrite the original log data. • The system shall integrate with a trusted **NTP (Network Time Protocol) source** to maintain accurate and synchronized timestamps across all logs and reports.		
11	The log server solution must be deployed on adequately sized hardware to ensure seamless log collection and forwarding to the SOC SIEM for all in-scope devices. The hardware configuration must include sufficient headroom beyond the baseline required for log collection alone, to handle increased utilization after SIEM integration.		
12	The proposed Log Server solution shall support industry-standard cryptographic mechanisms, in coordination with other integrated devices and systems, to ensure confidentiality, integrity, and authenticity of log data during transmission and storage. The solution shall provide secure encryption of log data in transit and at rest, tamper detection or prevention mechanisms, and protection against unauthorized modification, deletion, or corruption of logs.		
13.	All software, patches, or updates to be installed on the Log server system must be verified for authenticity and integrity through digital signature or checksum validation or any equivalent verification mechanism before patch installations. Verification may leverage OS-level or OEM-provided mechanisms to ensure trusted component deployment.		
14	The Log Server solution shall support centralized, role-based administrative access by integrating with the project's AAA system (e.g., RADIUS,TACACS+,LDAP,LDAPS,AD) for authentication and authorization.		

B. Type of logs-

The proposed Log Server solution shall capture and store logs from all relevant network and security components. The following are the minimum mandatory log types (but not limited to) that must be supported. It shall comply with ISO/IEC 27001:2022 controls and applicable CERT-In guidelines on log management, retention, and integrity.

SL no		Compliance (Yes/No)	Remarks
1	**SD-WAN Devices:** Firewall Logs, Intrusion Prevention System (IPS) Logs, VPN Logs, User Access Logs, Administrative Audit Logs, Application Control Logs, threat Intelligence / threat Detection Logs, System and Configuration Change Logs.		
2	**SD-WAN Controller:** Device Onboarding / De-registration Logs, Centralized Policy Change Logs, Administrative Access and Audit Logs, Control Plane Communication Logs, High Availability / Failover Logs, Firmware / Software update logs		
3	**Managed Switches:** Informational-Level Syslog Messages, Port Security, Configuration Change Logs, Firmware / Software Updates, Administrative Access logs.		
4	Switch Controller: Device Onboarding / De-registration Logs, Centralized Policy Change Logs, Administrative Access and Audit Logs, High Availability / Failover Logs, Firmware / Software Update logs.		
5	**Wi-Fi Access Points (12 units):** Authentication Logs (User & Device), Session Association / Disassociation Logs, Access Control / Policy Enforcement Logs.		
6	Wi-Fi Controller: Configuration Change and Policy Enforcement Logs, Administrative Access and Audit Logs, Radio Resource Management / Interference Detection Logs.		
7	NAC – access Control Logs (Authentications), Network Device Logs, Endpoint Compliance Check Logs, **Posture Validation Logs (Passed/Failed/Quarantine results with reason codes)**; AAA- all authorization, authentication, accounting, Administrative logs of users and devices to be captured along with audit logs of AAA device.		

Annexure-T-11

Virtual Lab Environment- Technical Annexure – Compliance Table

Sl. No.	Technical Requirement	Compliance (Yes/No)	Remarks
1	The virtual Lab based on EVE-NG Professional/Corporate Edition or equivalent enterprise-grade emulator		
2	The Virtual Lab topology/config file shall include the following minimum virtual components: a. 1no. SD-WAN Controller (production-equivalent) b. 10 nos. SD-WAN Edge devices using valid OEM-supplied images c. 6 nos. WAN emulation routers with WAN condition emulation support for ILL/MPLS links d. 10 nos. L2/L3 virtual switches that can support as is config for provided switches e. 10 nos. PC/endpoint nodes f. 2 nos. DNS/DHCP servers and 02 Root CA servers g. Optional (Simulated or near-functional Switch Controller, WIFI Controller/AAA/other supporting services only if OEM provided virtual image is available)		
3	All above components shall operate together with full, near-real configurations across all devices in a single production lab topology/configuration file, supporting real or near-real production workflows without any slowness, performance degradation, or instability. In addition, the Virtual Lab shall support a separate training/development configuration file that can run in parallel for testing, experimentation, and administrator training without impacting the production-equivalent lab topology.		
4	The Bidder shall size and provide all necessary compute, storage, hypervisor resources, and software/licenses, images to ensure that all required components and configurations operate seamlessly at all times. If any performance, capacity, or compatibility issues arise at any stage, the Bidder shall upgrade the hardware, software, or platform resources at no additional cost to the Purchaser.		
5	The lab shall support configuration validation, integration testing, troubleshooting, and testing, training with appropriate role-based access controls.		
6	Lab shall remain isolated from production but must fully replicate real or near-real production workflows for all above-mentioned devices.		

7	All required virtual images, hypervisor packages, platform licenses (EVE-NG), and OEM image licenses must be provided by the Bidder		
8	Backup/restore for lab configurations, snapshots, and virtual images must be provided		
9	Detailed documentation, user guides, and topology diagrams must be provided by the Bidder		
10	Any configuration changes related to SD-WAN, switches, or any other devices included in the Virtual Lab shall be first implemented, validated, and tested in the lab environment before being applied to production systems.		
11	The Bidder shall provide full support from project initiation to completion, including all required hardware, software, licenses, virtual images, platform subscriptions, and resources necessary for the uninterrupted operation of the Virtual Lab.		
12	An initial Virtual Lab setup with basic connectivity shall be demonstrated, including at least two SD-WAN edge devices, one SD-WAN Controller, two switches, PC/endpoints, and two WAN links. This baseline topology shall be operational before delivery, and detailed configurations shall be progressively updated in the lab as the project configuration evolves.		

Annexure-T-12

Technical Compliance Sheet: Rack for Network Equipment

This compliance sheet defines the minimum technical requirements for a 9U network equipment rack suitable for hosting one SD-WAN device, one 24-port L2 Managed Switch, two WAN link devices (modems), power distribution equipment, cable management modules, and associated accessories. The rack must support secure, well-ventilated installation with adequate space for future expansion and maintenance accessibility.

Sl. No.	Technical Specification	Compliance(Yes/No)	Remarks
1	Rack height must be minimum 9U, 19-inch standard width, compliant with ANSI/EIA RS-310-D and suitable for mounting standard rack-mountable devices.		
2	Must support mounting of standard 1U rack devices (SD-WAN, Switch, Power Units) and shelf-based installation for non-rackable devices (e.g., modems, ONTs).		
3	Rack must include at least one universal vented equipment shelf (1U) capable of securely holding two WAN link devices and other small peripherals.		
4	Rack must include minimum one 1U horizontal cable manager with D-rings or brush panel for structured cable routing. Vertical cable management support is preferable.		
5	Rack must provide passive ventilation and support installation of optional fan tray (active ventilation) when required based on environmental conditions.		
6	Rack must be wall-mounted or floor-standing, with a lockable transparent/metal front door, and removable/hinged side panels to support maintenance.		
7	Rack body must be made of steel/CRCA, powder-coated, corrosion-resistant, with a minimum load capacity of 40 kg.		
8	Must include 1 × 6-socket surge-protected power strip (Indian plug type) with mounting brackets for internal installation.		
9	Must include a grounding/earthing kit, along with standard M6 mounting hardware (screws, cage nuts, washers).		
10	Rack should include optional 1U blank panels/filler plates for airflow control and aesthetic completion.		
11	Rack should provide adequate depth (minimum 400–450 mm usable depth) to support SD-WAN devices and power units with safe cable bend radius.		
12	Rack should support rear cable entry and top/bottom knockouts for power and link cable routing.		
13	Rack should include labelling provisions for equipment identification and cable management.		

Annexure-T-13

Documentation Compliance

All the following documents are mandatory and must be submitted in editable format and signed PDF. Go-Live (start of warranty/maintenance) will be allowed only after all documents (SL no 1-13) are received, verified, and approved. All documents shall follow ISO/IEC 27001:2022 standards, including proper versioning, author/approver details, change history, controlled distribution, and updates whenever any configuration/device/user change occurs.

Documentation Compliance Table

Sl. No.	Document / Deliverable	Description / Requirements	Compliance (Yes/No)	Remarks
1	Network Architecture Diagrams (Pre & Post)	Before-and-after diagrams for DC, DR, HQ, ALDC, and one sample site office (as decided by WBSEDCL) showing device placement, links, routing, DMZ, VLAN segmentation.		
2	IP Addressing & Allocation Document	Full IP plan including LAN/WAN subnets, DHCP pools, loopbacks, free IP pools, and per-site allocations for all locations.		
3	Failover, Redundancy & High Availability Operations Document	HA architecture, DR shift steps, device/server failover behaviour, SD-WAN tunnel failover, and testing workflows for all devices and servers working in failover mode in DC and DR.		
4	Device & Server Configuration Records	Full configuration snapshots of all devices in this project in DC, DR, HQ, ALDC and one site office with explanations and annotations.		
5	Internet Access & Authentication Flow Document	NAC posture, LDAP/AD integration, authentication flow, breakout routing, firewall traversal, logging behaviour.		
6	Unified Routing & SD-WAN Policy Document	Routing strategy, redistribution, SD-WAN traffic steering, application-based routing, link priority rules, protocols used etc.		
7	Virtual Lab Documentation (EVE-NG or Equivalent)	Lab topology, VM list, near-production configurations, configuration files, usage procedures, and access details.		
8	Patch Management & Software Lifecycle Document	Patch policy, process to be followed, for all devices in this project. Device wise patch management process documentation.		

9	Operational SOPs & Administrative Manuals	The bidder shall provide detailed Operational Standard Operating Procedures (SOPs) for all devices in this project covering all routine and critical activities required for the day-to-day management of the deployed solution. At minimum, the SOPs must include clear, step-by-step procedures for: • **How to monitor devices** (health status, alerts, logs, performance counters). • **How to take backups** of all relevant device and controller configurations. • **How to restore a configuration** in case of failure, corruption, or rollback. • **How to troubleshoot link-down scenarios**, including diagnostic commands and escalation triggers. • **How to escalate issues** within the defined support hierarchy and escalation matrix. • **How to handle alarms**, including identification, containment, resolution, and documentation.		
10	Administrative Access, Users & Role Management Document	The bidder shall provide a complete record of all **admin/users with configuration edit access** across every device and system in this project. The document must clearly list the **number of such users, their user IDs, assigned roles/privilege levels, and the department or individual to whom each account is mapped**. It must also specify the authentication method used (LDAP,LDAPS,AD,TACACS+,RADIUS or local)**,** the enforced password/MFA policies, and the logging and audit mechanisms that record and trace all administrative/configuration actions. Additionally, the document shall include the approved procedures for creation, modification, removal, and credential recovery for all admin/config-edit users.		
11	OEM Device Specification Sheets / Data Sheets	Official OEM datasheets for all devices in this project showing model, features, capacities, compliance, supported protocols, and firmware support lifecycle.		
12	Asset Register & Inventory Documentation	The Bidder shall maintain and submit a detailed Asset Register containing details of all devices supplied and deployed under this project, aligned with ISO/IEC 27001:2022 asset-management requirements. The Asset Register shall be maintained in Excel format and updated progressively throughout the project,		

		including initial submission at delivery milestones and subsequent updates whenever devices are installed, moved, replaced, or decommissioned. It shall include, at minimum: Asset Type, Brand, Model, Serial Number, Device Role, Location, IP Address, MAC Address, Firmware/Software Version, License Details, EOS/EOL Dates, Installation Date, Owner/Custodian, and Remarks. The Bidder's L2 onsite personnel shall be responsible for maintaining and updating this register in coordination with the WBSEDCL.		
13	Final Master Documentation Package	A consolidated, indexed, and version-controlled set (hard copy and soft copy) of all required documentation, (Sl. no 1-12 here and as in scope of work) compiled into a single comprehensive package. The documentation shall follow ISO/IEC 27001:2022 formatting standards, including author details, version numbers, update dates, and complete revision history for every document requested above.		
14	Documentation Refresh and Update Requirements	The bidder shall provide refreshed and updated versions of all documentation listed above, including the Final Master Documentation Package, on an annual basis and immediately after any major change in configuration, devices, network architecture, security policies, or administrative/user access. WBSEDCL reserves the right to request updated documentation at any time during the contract period if significant changes occur or for audit and compliance purposes. The bidder shall provide such updated documentation promptly and without any additional cost or delay. DR drill and Backup and Recovery documentation.		

Annexure-T-14

NOC Display, Monitoring PC & Accessories Technical Compliance Sheet

Section A: Display Units & Floor Stand – Technical Requirements & Compliance

Sl. No.	Requirement	Compliance (Yes/No)	Remarks
1	Three (3) 65-inch and Two (2) 55-inch 4K UHD commercial-grade displays.		
2	Commercial/Industrial Grade LED/IPS/VA panel with anti-glare, high-contrast capability.		
3	Brightness: ≥500 nits (65-inch), ≥450–500 nits (55-inch), with native 60 Hz refresh rate. Display must support clear visibility at a 4–6 meter viewing distance.		
4	24×7 continuous-rated panel durability. The display shall include burn-in protection and pixel-shift technology to prevent image retention. The bidder shall replace the display at no cost if any pixel burn-out, bright/dead pixel, spot, or visual artefact appears at any time during the project period.		
5	Required Ports: Minimum 2×HDMI, USB ports, and LAN port for remote monitoring. The display must support LAN-based remote monitoring and OSD control to allow authorised personnel to remotely power ON/OFF, change input sources, adjust settings, monitor panel health, and perform diagnostics without physically accessing the screen.		
6	Must support GUI dashboards at minimum for SD-WAN, Managed Switch, NAC-AAA, Logs & Reports required in this project.		
7	Must support multi-window split (OS-based or PIP/PBP).		
8	Must provide stable GUI rendering without jitter or latency when dashboards are accessed from any WBSEDCL location in West Bengal over MPLS links with sufficient bandwidth.		
9	5 nos. Heavy-duty pedestal floor stand, ensuring proper fit- VESA compatible (Video Electronics Standards Association), per stand ≥60 kg load bearing capacity. The structure must guarantee long-term stability, provide appropriate height adjustment capabilities, and incorporate safety features to prevent tipping or failure and must be able to hold the above displays continuously and safely at appropriate height as per requirement.		
10	Complete installation, alignment, fixing and cable management shall be carried out by the bidder.		

11	OEM Technical Datasheet must be submitted for verification. Display units must comply with BIS (India), CE, FCC and EMI/EMC safety certifications to ensure electrical, thermal and electromagnetic safety in the NOC environment.		
12	5-year comprehensive onsite warranty/maintenance for all displays, parts, stands and accessories.		
13	Bidder shall provide all cabling, ducting, clamps, mounting hardware, software, utilities or applications required for display installation and operation.		
14.	Only electrical power points will be provided by WBSEDCL. All power connectors/adapters required for displays shall be supplied by the bidder. The bidder shall supply BIS-certified surge protectors/spike guards and ensure safe power connectivity for all displays and PCs. Any damage due to electrical surges, spikes or fluctuations—despite grounding provided by WBSEDCL —shall be treated as bidder's responsibility, and warranty claims shall not be denied on the basis of power fluctuation.		

Section B: Mini-PC Requirements & Compliance

Sl. No.	Requirement	Compliance (Yes/No)	Remarks
1	One Mini-low noise PC for each display (5 units in total for 5 displays).		
2	Minimum Specification (higher specification to be supplied if required for smooth dashboard rendering): • Processor: Intel Core i5 (12th Gen or higher) / AMD Ryzen 5 (5000 series or higher) • RAM: Minimum 16 GB • Storage: Minimum 500 GB NVMe SSD • Graphics: Integrated GPU capable of smooth multi-dashboard 4K output • Ports: HDMI 2.0 / DP 1.4 supporting 4K@60Hz • Low-Noise Operation: <30 dB typical Must support simultaneous display of: (a) two (2) live dashboards (SD-WAN & Managed Switch) in split-screen mode, and (b) at least three (3) dashboards in background (NAC-AAA, Log Server, Report Analytics). Performance must not degrade after dashboard upgrades during the entire project period.		
3	Windows 11 Pro (licensed) with all required software and browser compatibility. To be updated as per latest in support OS during full project timeline. No EOS OS to be used any time during project period. Updated patch to be maintained.		
4	Auto-load dashboards on startup via Startup Folder / Task Scheduler. If system restarts, dashboards must reopen automatically in correct layout		
5	The bidder shall supply high-quality wireless keyboard and mouse sets for each display and associated compact PC. The wireless peripherals must		

	support a reliable operational range of at least 8 meters without signal drop, latency, jitter, or input delay, ensuring smooth control of dashboards displayed on large 55-inch and 65-inch screens. Devices shall use robust 2.4 GHz or equivalent interference-resistant wireless technology suitable for NOC environments, where multiple wireless devices may operate simultaneously.		
6	5-year comprehensive onsite warranty/maintenance during project period for PC and accessories in this project.		
7	Mini-PC must support OS hardening, browser hardening and restriction of local admin privileges as per WBSEDCL security policy.		
8	Mini-PC must integrate with the NAC-AAA infrastructure and Log Server used in this project, ensuring that all relevant events from the Mini-PCs are captured, forwarded, and retained for audit, troubleshooting and compliance.		
9	Bidder must ensure compatibility of display screen and Mini-PC hardware/software with all dashboard updates of SD-WAN, Switching, NAC/AAA, Logs and Reporting solutions during the entire project period.		
10	OEM Technical Datasheet must be submitted for verification.		
11	All required accessories—including batteries, USB wireless receivers, HDMI/DisplayPort cables for TV-to-PC connectivity, LAN cables, power adapters, extension connectors, cable-management materials, and any additional PC-related accessories needed for full functionality—shall be supplied by the bidder. All supplied HDMI/DP and LAN cables must be of sufficient length to support stand-mounted display placement. Bidder shall ensure proper surge protection and safe electrical connectivity for all PCs and display interfaces		

BID PROPOSAL

From:

Bidder's Name and Address :

Contact person :

Designation :

Telephone No. - :

Fax :

Tender Reference :

To
The Chief Engineer,
IT Cell,
West Bengal State Electricity Distribution Company Limited,
3rdFloor, Block-'C' & 'D', VidyutBhavan,
Bidhannagar,
Kolkata- 700091

Sub- Invitation to bid for Implementation of SD-WAN, Managed Switch and Network Upgradation under WBSEDCL

Dear Sir,

1. We the undersigned Bidder/(s), having read and examined in details the specifications and other documents of the subject Tender, do hereby propose to execute the contract as per specification as set forth in your Bid-Document. We have read and examined in details all the clauses mentioned in NIT including representative of the vendor,LD,PBG,Additional PBG,SoW etc. and unconditionally agree with the same.

a) PRICES AND VALIDITY :

i. The offer against tender will remain valid for a minimum period 180 (one hundred eighty) days from the next day of opening of the tender. We further declare that prices stated in our proposal are in accordance with your bidding and the quoted unit rates will remain firm throughout the period of the contract.

ii. GST and/or any other applicable tax in lieu of GST as per law of land and other Levies, if any, applicable on transaction from us to you payable extra by you against production of documentary evidence to be submitted by us. GST and/or any other applicable tax in lieu of GST as per law of land shall be payable on over or above the quoted rate as applicable value and at prevailing rate.

b) BID GUARANTEE :

We have enclosed a Bid Guarantee in the form of Bank Guarantee from ……drawn in favour of WBSEDCL/paid through online mode for an amount of Rs.....

c) CONTRACT PERFORMANCE GUARANTEE AND ADDITIONAL CONTRACT PERFORMANCE GUARANTEE :

We further agree that if our proposal is accepted, we shall provide a Contract Performance Guarantee of value, equivalent to three percent (3%) of the Contract Price as stipulated in Bid document in the form of Bank Guarantee (Please specify the form of guarantee) in your favour and enter into a formal agreement with you within 30 (Thirty) days from the date of placement of Letter of Award. Additionally, if applicable, we shall provide an additional Contract Performance Guarantee equivalent to 10 (ten) % of tendered amount as per terms and conditions stipulated in NIT.

Dated.....this.....day of.....2022

Thanking you, we remain,

Yours faithfully,

Date _____

Place _____ (Signature) _____

(Printed Name) _____

(Designation) _____

(Common Seal) _____

Business Address:
Name & Address of Authorized Signatory:

Annexure-II

Bid Details

(Instruction: It will be treated as reference for technical evaluation of bid. Incomplete or improperly submitted bid detail may lead to rejection of bid.)

Sl. No	Power of Attorney from Bidder		Page No in technical Proposal
1	Name of the Bidder (Company Name)		
2	Power of Attorney (on non-judicial stamp paper of appropriate value)		
3	Person Issuing Power of Attorney		
4	Signing Authority/Person for this bid		

Sl. No	Correspondence Details (will be used for communications related to this NIT)		Page No in technical Proposal
1	Email Id		
2	Mobile No		
3	Correspondence Address		

Sl. No	Payment Confirmation for EMD (Earnest Money Deposit)		Page No in technical Proposal
1	**Payment Mode (NEFT/RTGS/E-Challan/Bank Guarantee)**		
2	**UTR No/ Challan No/BG Number**		
3	**Scanned Copy (Payment Receipt)**		
4	**BG Details (will be used confirmation of BG from Issuing bank) as per Annexure -V**		
	i. Scanned Copy of BG		
	ii. BG Number		
	iii. BG Issue Date		
	iv. Issuing Bank Name		
	v. IFSC of Issuing Bank		
	vi. Email Id of Contact Person from Issuing bank for Confirmation of BG		

Signed Documents as per NIT and corresponding Annexures with Seal of Bidder			
Sl. No	**Document Details**	**Submission Status (Yes/No)**	**Page No in technical Proposal**
1	Signed Copy of Complete NIT with Annexures		
2	Signed Copy of Addenda/Corrigendum, if any		
3	Signed Copy of properly filled Bid Proposal as per Annexure-I		
4	Signed Copy of properly filled Bid Details as per Annexure-II		
5	Signed Copy of properly filled Mandatory Conditions mentioned in Annexure –XI		
6	Signed Copy of properly filled Non Disclosure Agreement as per Annexure IX		
7	Signed Copy of properly filled Contract Agreement as per Annexure X		
8	Signed copy of technical annexure T-1 to T-14 by bidder and OEM's		

Legal Details of the Company			
Sl. No	**Document Name**	**Number**	**Page No in technical Proposal**
1	**Corporate Identification Number (CIN)**		
2	**PAN**		
3	**GST Registration No**		

Financial Statements - Balance Sheet			
Sl. No	**Financial Year**	**Net Worth (in Lakh INR)**	**Page No in technical Proposal**
1	2024-25		
2	2023-24		
3	2022-23		

Financial Statements - Profit & Loss Statement			
Sl. No	**Financial Year**	**Turn Over (in Lakh INR)**	**Page No in technical Proposal**
1	2024-25		
2	2023-24		

3	2022-23		

CA Certificate for Net Worth			
Sl. No	**Financial Year**	**Net Worth (in Lakh INR)**	**Page No in technical Proposal**
1	2024-25		
2	2023-24		
3	2022-23		

Income Tax Return			
Sl. No	**Financial Year**	**Submission Status (Yes/No)**	**Page No in technical Proposal**
1	2024-25		
2	2023-24		
3	2022-23		

GST Return			
Sl. No	**Financial Year**	**Submission Status (Yes/No)**	**Page No in technical Proposal**
1	2024-25		
2	2023-24		

Annexure-III

PROFORMA FOR BANK GUARANTEE
FOR BID GUARANTEE (EMD)
(To be stamped in accordance with Stamp Act)

Ref. No.: Date:

To

The Chief Engineer,
IT Cell,
West Bengal State Electricity Distribution Company Limited,
3rd FLOOR, 'C' & 'D'- BLOCK, Vidyut Bhavan,
DJ Block, Sector – II,
Salt Lake, Bidhannagar,
Kolkata- 700 091.

Dear Sirs,

In accordance with your Notice Inviting e-Tender (NIeT) under your Specification No._____ M/s _____ having its Registered Head Office at _____ (hereinafter called the Bidder) wish to participate in the said Tender for _____.

As an irrevocable Bank Guarantee against Bid Guarantee for an amount of ____ is required to be submitted by the Bidder as a condition precedent for participation in the said Tender, which amount is liable to be forfeited on the happening of any contingencies mentioned in the Tender Documents.

We, the _____ Bank at _____ having our Head Office at _____ (Address of Bank) guarantee and undertake to pay immediately on demand by West Bengal State Electricity Distribution Company Ltd.(WBSEDCL) the amount of _____ (in words and figures) without any reservation, protest, demur and recourse. Any such demand made by said Purchaser shall be conclusive and binding on us irrespective of any dispute of difference raised by the Bidder.

This Guarantee shall be irrevocable and shall remain valid uptothe period **of 180 (one hundred and eighty) days from the date of opening Technical Proposal**. If any further extension of this guarantee is required, thesame shall be extended to such required period on receiving instructions from M/s _____ on whose behalf this Guarantee is issued.

All rights of West Bengal State Electricity Distribution Company Ltd.(WBSEDCL) under this Guarantee shall be forfeited and the Bank shall be relieved and discharged from all liabilities there under unless WBSEDCL brings any suit or, section to enforce a claim under this Guarantee against the Bank within six months from the above mentioned expiry date of validity or, from that of the extended date.

In witness whereof the Bank, through its authorised Officer, has set its hand and stamp on this _____ day of _____ 20 ___ at _____.

WITNESS :

_____ _____
(Signature) (Signature

_____ _____
(Name) (Name)

_____ _____
(Official address) (Designation with Bank Stamp)

Attorney as per Power of Attorney No. _____
Date _____

@ This date should be initially for one hundred eighty (180) days and may be extended from time to time.

Annexure-IV

Statement of Deviation from Terms and Conditions of Bid Document

To,

The Chief Engineer,
IT Cell,
West Bengal State Electricity Distribution Company Limited,
3rdFLOOR, 'C' & 'D'- BLOCK, VidyutBhavan,
DJ Block, Sector – II,
Salt Lake,Bidhannagar,
Kolkata- 700 091.

Reference: NIeT No ……Dated…….

Sir,

There are no deviations (null deviations) from the terms and conditions of the Bid document. All the terms and conditions and all other clausesof the Bid document are acceptable to us.

Signature _____

Name:

Designation:

Date:

Annexure-V

PROFORMA FOR BANK GUARANTEE FOR CONTRACT PERFORMANCE
(To be stamped in accordance with Stamp Act)

Bank Guarantee No._____

Ref No._____ Date: _____

To

West Bengal State Electricity Distribution Company Limited,
3rd FLOOR, 'C' & 'D'- BLOCK, Vidyut Bhavan,
DJ Block, Sector – II,
Salt Lake, Bidhannagar,
Kolkata- 700 091.

Dear Sirs,

In consideration of West Bengal State Electricity Distribution Company Ltd (hereinafter referred to as WBSEDCL) which expression shall unless repugnant to the context or meaning thereof include its successors, administrators and assigns having awarded to M/s _____ with its Registered/Head Office at _____(hereinafter referred to as the 'Contractor') which expression shall unless repugnant to the context or meaning thereof, include its successors, administrators, executors and assigns, a Contract by issue of Letter of Award No./Order No. _____ dated_____ valued at_____ for_____ (Scope of Contract) and the Selected bidder(s) having agreed to provide a Contract Performance Guarantee of Rs. _____for the faithful performance of the contract. We _____(Name and Address) having its Head Office at_____ hereinafter referred to as the `Bank') which expression shall, unless repugnant to the context or meaning thereof include its successors, administrators, executors and assigns do hereby guarantee and undertake to pay WBSEDCL, on demand any and all moneys payable by the Contract to the extent of _____as aforesaid at any time upto (day/month/year) without any demur, reservation, contest recourse or protest and or without any reference to the Selected bidder(s). Any such demand madeby WBSEDCL on the Bank shall be conclusive and binding notwithstanding any difference between WBSEDCL and the Selected bidder(s) or any dispute pending before any Court, Tribunal or any other Authority. The Bank undertakes not to revoke this guarantee during its currency without previousconsent of WBSEDCL and further agrees that the guarantee herein contained shall continue to be enforceable till the WBSEDCL discharges this guarantee.

WBSEDCL shall have the fullest liberty without affecting in any way the liability of the Bank under this guarantee from time to time extend the time for performance of the Contract by the Selected bidder(s). WBSEDCL, shall have the fullest liberty, without affecting this guarantee to postpone from time to time the exercise of any powers vested in them or of any right which they might have against the Selected bidder(s) and to exercise the same at any time and any manner, and either to enforce or to forbear to enforce any covenants, contained or implied in the Contract between WBSEDCL and the Selected bidder(s) or any other course of remedy or security available to WBSEDCL. The Bank shall not bereleased of its obligations under this presents by any exercise by WBSEDCL of its liberty with reference to the matters aforesaid or any of them or by reason or any other acts of omission or commission on the part of WBSEDCL or any other indulgence shown by WBSEDCL or by any other matter or thing whatsoever which under the law would but for these provisions have the effect of relieving the Bank.

The Bank also agrees that WBSEDCL at its option shall be entitled toenforce this guarantee against the Bank as a Principal debtor, in the first instance without proceeding against the Selected bidder(s) and notwithstanding any security or other guarantee that WBSEDCL may have in relation to the selected bidder(s)'s liabilities.
Notwithstanding anything contained herein above our liability under this guarantee is restricted to_____ and shall remain in force upto and including_____ and shall be extended from time to time for such period, as may be desired by M/s._____ to whose behalf this guarantee has been given.

All rights of WBSEDCL under this guarantee shall be forfeited and theBank shall be relieved and discharged from all liabilities there under unless the WBSEDCL brings any suit or section, to enforce a claim under this guaranteeagainst the Bank within six months from the above-mentioned date or from the extended date.
Dated this _____day of_____20 ___ at _____

Witness:

_____ _____
(Signature) (Signature)

_____ _____
(Name) (Name)

_____ _____
(Official address) (Designation with Bank Stamp)

_____
Attorney as per Power of

Attorney No._____ Date

Annexure-VI

FORMAT OF THE BANK GUARANTEE FOR ADDITIONALPERFORMANCE SECURITY DEPOSIT

To
The Chief Engineer, IT Cell, WBSEDCL
3rd floor, D Block, Vidyut Bhavan
DJ Block, Sector – II, Salt Lake, Kolkata - 700 091

WHEREAS……. (name and address of "the Contractor") Contractor) (hereafter called "the Contractor") has undertaken, in pursuance of Contract no. ……. Dated……. to execute……. (name of Contract and brief description of Works (hereinafter called "the Contract").
AND WHEREAS it has been stipulated by you in the said Contract that the Contractor shall furnish you with a Bank Guarantee by a Scheduled Commercial Bank for the sum specified therein for 'ADDITIONAL PERFORMANCE SECURITY DEPOSIT' for compliance with his obligation in accordance with the Contract;

NOW WHEREAS we……..(indicate the name of the bank and branch) have agreed to give the Contractor such a Bank Guarantee.

NOW THEREFORE we……. (indicate the name of the bank & branch) hereby affirm that we are the Guarantor and responsible to you
on behalf of the Contractor, upto a total of Rs. .....(amount of guarantee) ……..(in words). We undertake to pay you, upon your first written demand and without cavil of argument, a sum within the limits of……(amount of guarantee) as aforesaid without your needing to prove or to show grounds or reasons for your demand for the sum specified therein.

We ……. (indicate the name of the bank and branch) hereby waive the necessity of your demanding the said debt from the contractor before presenting us with the demand.

We…… (indicate the name of the bank and branch) further agree to pay to you any money so demanded notwithstanding any dispute or disputes raised by the contractor(s) in any suit or proceeding pending before any court or Tribunal.....the present absolute and unequivocal.
The payment so made by us under this bond shall be a valid discharge of our liability for payment there under and the contractor(s) shall have no claim against us for making such payment, We (indicate the name of the bank and branch) further agree that no change or addition to or other modification of the terms of the Contract or of the works to be performed there under or of any of the Contract documents which may be made between you and the Contractor shall in any way release us from any liability under this guarantee, and we hereby waive notice of any such change, addition or modification.
We…… (indicate the name of the bank and branch) lastly undertake not to revoke this guarantee except with the previous consent of you in writing.
This Guarantee shall be valid upto…..... it comes into force with immediate effect and shall remain in force and valid for a period upto the time of completion of the work under the stated contract plus claim period of Six months for the Bank Guarantee. Notwithstanding anything mentioned above our liability against this guarantee is restricted to Rs…….. (Rupees.) and unless a claim in writing is lodge if with us within the validity period i.e. upto……of this guarantee all our liabilities under this guarantee shall cease to exist.

Signed and sealed this ……..day . .....of 202…….at …….

SIGNED, SEALED AND DELIVERED
by:

For and on behalf of the BANK
(Signature)
(Name)
(Designation),
(Code Number),
Address

NOTEST (1) The bank guarantee should contain number of the officer(s) signing the guarantee. The address, telephone number and other details of the Head Office of the Bank as well as of issuing Branch should be mentioned on the covering letter issuing Branch.

Annexure-VII

Pre-BID Query Format (to be submitted in XLSX format only)

NOTE- Queries not submitted in the below format, or without reference to specific clause and page numbers, may not be considered.

Tender Reference no:
Name of the Bidder/OEM:
No. of Personnel's attending Pre Bid:

Sl. No.	Clause No of the Tender Document	Page No of the Tender Document	Text Details	Query Details	Justification of the Query	Remarks
1						
2						
..						
..						

Annexure -VIII

PRICE SCHEDULE (UNPRICED :Not to be quoted here)

Validate Print Help

Item Rate BoQ

Tender Inviting Authority: Chief Engineer,IT Cell, WBSEDCL.

Name of Work: Implementation of SD-WAN,Network Managed Switch and Network Upgradation under WBSEDCL.

Contract No:

Name of the Bidder/ Bidding Firm / Company :	

PRICE SCHEDULE

(This BOQ template must not be modified/replaced by the bidder and the same should be uploaded after filling the relevent columns, else the bidder is liable to be rejected for this tender. Bidders are allowed to enter the Bidder Name and Values only)

NUMBER #	TEXT #	NUMBER #	NUMBER #	DATE	NUMBER #	TEXT #
Sl. No.	Item Description	Quantity	BASIC RATE In Figures To be entered by the Bidder Rs. P		TOTAL AMOUNT Without GST	TOTAL AMOUNT without GST In Words
1	2	4	13		53	55
1	Items					

1.01	Supply,delivery and installation of SD-WAN Box Type-B1 with the necessary hardware,software,licenses.	4.000			**0.00**	INR Zero Only
1.02	5 years of post–go-live warranty and maintenance support for SD-WAN Box Type-B1.	4.000			**0.00**	INR Zero Only
1.03	Supply,delivery and installation of SD-WAN Box Type-B2 with the necessary hardware,software,licenses.	2.000			**0.00**	INR Zero Only
1.04	5 years of post–go-live warranty and maintenance support for SD-WAN Box Type-B2.	2.000			**0.00**	INR Zero Only
1.05	Supply,delivery and installation of SD-WAN Box Type-B3 with the necessary hardware,software,licenses.	2.000			**0.00**	INR Zero Only
1.06	5 years of post–go-live warranty and maintenance support for SD-WAN Box Type-B3	2.000			**0.00**	INR Zero Only
1.07	Supply,delivery and installation of SD-WAN Box Type-A1 with the necessary hardware,software,licenses.	692.000			**0.00**	INR Zero Only
1.08	5 years of post–go-live warranty and maintenance support for SD-WAN Box Type-A1	692.000			**0.00**	INR Zero Only
1.09	Supply,delivery and installation of SD-WAN Box Type-A2 with the necessary hardware,software,licenses.	50.000			**0.00**	INR Zero Only
1.1	5 years of post–go-live warranty and maintenance support for SD-WAN Box Type-A2	50.000			**0.00**	INR Zero Only
1.11	Supply,delivery and installation of 24 Port Managed Network Layer-2 Switch.	800.000			**0.00**	INR Zero Only
1.12	5 years of post–go-live warranty and maintenance support for 24 Port Managed Network Layer-2 Switch	800.000			**0.00**	INR Zero Only

1.13	Supply, delivery, and installation of SDWAN Controller along with adequate compute resources (CPU, memory, storage), software, and licenses.	2.000			**0.00**	INR Zero Only
1.14	5 years of post–go-live warranty and maintenance support for SDWAN Controller along with adequate compute resources (CPU, memory, storage etc.), software, and licenses.	2.000			**0.00**	INR Zero Only
1.15	Supply, delivery, and installation of Managed Switch Controller along with adequate compute resources (CPU, memory, storage etc.), software, and licenses.	2.000			**0.00**	INR Zero Only
1.16	5 years of post–go-live warranty and maintenance support for Managed Switch Controller along with adequate compute resources (CPU, memory, storage etc.), software, and licenses.	2.000			**0.00**	INR Zero Only
1.17	Supply, delivery, and installation of Wi-Fi Access Point along with adequate compute resources (CPU, memory, storage etc.), software, and licenses.	24.000			**0.00**	INR Zero Only
1.18	5 years of post–go-live warranty and maintenance support for Wi-iFi Access Point along with adequate compute resources (CPU, memory, storage etc.), software, and licenses.	24.000			**0.00**	INR Zero Only
1.19	Supply, delivery, and installation of Wi-Fi Controller along with adequate compute resources (CPU, memory, storage etc.), software, and licenses.	1.000			**0.00**	INR Zero Only
1.2	5 years of post–go-live warranty and maintenance support for Wi-iFi Controller along with adequate compute resources (CPU, memory, storage), software, and licenses.	1.000			**0.00**	INR Zero Only

1.21	Supply, delivery, installation, configuration, and commissioning of Network Access Controller (NAC) and AAA functionality, including adequate compute resources (CPU, memory, and storage), required software and licenses, support for agent-based and agentless devices, user authentication, and all features as specified in the Technical Specifications.	2.000			**0.00**	INR Zero Only
1.22	5 years of post–go-live warranty and maintenance support for Network Access Controller (NAC) and AAA functionality, including adequate compute resources (CPU, memory, and storage), required software and licenses, support for agent-based and agentless devices, user authentication, and all features as specified in the Technical Specifications.	2.000			**0.00**	INR Zero Only
1.23	Supply, delivery, and installation of Log Server Solution along with adequate compute resources (CPU, memory, storage), software, and licenses.	2.000			**0.00**	INR Zero Only
1.24	5 years of post–go-live warranty and maintenance support for Log Server Solution along with adequate compute resources (CPU, memory, storage), software, and licenses.	2.000			**0.00**	INR Zero Only
1.25	Supply, delivery and installation of Reporting & Analytics solutions along with adequate compute resources (CPU, memory, storage), software, and licenses.	2.000			**0.00**	INR Zero Only
1.26	5 years of post–go-live warranty and maintenance support for Reporting & Analytics solutions along with adequate compute resources (CPU, memory, storage), software, and licenses.	2.000			**0.00**	INR Zero Only
1.27	Supply, delivery and installation of Virtual Lab. solution along with adequate compute resources (CPU, memory, storage), software, and licenses.	1.000			**0.00**	INR Zero Only

1.28	5 years of post–go-live warranty and maintenance support forVirtual Lab. Solution along with adequate compute resources (CPU, memory, storage), software, and licenses.	1.000			**0.00**	INR Zero Only
1.29	Supply, delivery and installation of Client VPN (ZTNA) – 200 nos. concurrent users licenses for 5 years from Post-go-live period	1.000			**0.00**	INR Zero Only
1.3	Supply, delivery and installation of 9U Network Rack	100.000			**0.00**	INR Zero Only
1.31	Supply, delivery and installation of 55-inch 4K UHD commercial-grade display with Heavy-duty pedestal floor stand	2.000			**0.00**	INR Zero Only
1.32	5 years of post–go-live warranty and maintenance support for 55-inch 4K UHD commercial-grade display with Heavy-duty pedestal floor stand	2.000			**0.00**	INR Zero Only
1.33	Supply, delivery and installation of 65-inch 4K UHD commercial-grade display with Heavy-duty pedestal floor stand	3.000			**0.00**	INR Zero Only
1.34	5 years of post–go-live warranty and maintenance support for 65-inch 4K UHD commercial-grade display with Heavy-duty pedestal floor stand	3.000			**0.00**	INR Zero Only
1.35	Supply, delivery and installation of mini PC wth Keyboard,mouse	5.000			**0.00**	INR Zero Only
1.36	5 years of post–go-live warranty and maintenance support for mini PC wth Keyboard,mouse	5.000			**0.00**	INR Zero Only
Total in Figures					**0.00**	INR Zero Only
Quoted Rate in Words		**INR Zero Only**				

Annexure-IX

NON-DISCLOSURE CERTIFICATE

(To be executed on non-Judicial stamp paper of Rs. 100)

Ref.- **Date-**

To
The Chief Engineer
IT & C Cell, D Block,
Vidyut Bhavan.,
Block-DJ, Sector-I, Kolkata- 700091

Dear Sir(s)

……..(Name of Vendor) [hereinafter referred to as 'Our', 'We' and Us'] hereby confirm the terms of our certificate i.r.o confidentiality and non-disclosure of the information to others which WBSEDCL will be making available to us.

WBSEDCL will provide us access to the office premises, network equipment, security devices, associated infrastructure, and all relevant technical and operational information required for execution of this project..

The information may be disclosed to us either in writing or by access to systems or devices or raw data/information. In consideration for WBSEDCL granting this access to the information…… (Name of Vendor) agrees that

1. Subject to clause No. 7 below, we will keep the information strictly confidential and will not disclose it to any third party (other Vendor/Agency/ Bidder or its staff/ media authority / individual/ Company/organization) or any party/person not involved in this project in any form without prior written consent of WBSEDCL.

2. The devices, there configuration or any other WBSEDCL office related information or data will only be disclosed to those personnel of the Vendor who necessarily require or need to know it for the proper performance of their duties/execution of works in relation to this project and then also to the extent reasonably necessary. We will take appropriate steps to ensure that all personnel to whom access to the information is given are aware of its confidentiality.

   Where troubleshooting requires support from the respective OEM, we may share only the minimum technical information necessary through the OEM's approved secure channels. We accept full responsibility for ensuring that the OEM maintains confidentiality and does not use or disclose the information beyond the purpose of issue resolution.

3. The information disclosed to us by WBSEDCL will be used solely for the purpose of execution of this project.

4. We shall comply with the confidentiality and/or obligations set out herein above since inception of the LOA, till the completion of the project and shall share the same only to the authorized personnel of WBSEDCL. We hereby declare that we will not store, upload, transfer, or process WBSEDCL's confidential information on any external cloud platform, AI tool, or third-party system unless expressly approved in writing by WBSEDCL.

5. The confidentiality shall be maintained during and even after the completion of this project and shall only furnish details upon receipt of written instruction of WBSEDCL. We shall store and handle WBSEDCL's confidential information using industry-standard security controls, including role-based access, encryption, and restricted storage. In the event of any actual or suspected breach of confidentiality, we shall immediately notify WBSEDCL and fully cooperate in all investigation and mitigation measures, in accordance with applicable Government of India laws and prescribed data-protection requirements.

6. Upon completion or termination of our involvement in this project, and upon receiving written instructions from WBSEDCL, we shall return all information disclosed to us or generated by us within a reasonable period. Except for retention of professional records strictly required by law, we shall securely delete all remaining confidential information. We further certify that all soft copies, backups, logs, configurations, extracted data, and any derivative information have been permanently destroyed in accordance with WBSEDCL's instructions. WBSEDCL shall have the right to verify compliance with confidentiality obligations, including destruction of information, through audit or written confirmation.

7. The obligation contained above shall not apply to any information which

i. is or becomes publicly available (otherwise than through a breach of this certificate)
ii. is already in vendor's possession without any obligation of confidentiality.
iii is obtained by vendor from a third party without any, obligation of confidentiality.
Iv is independently developed by vendor outside the scope of this certificate.
v. Vendor is required to disclose by any legal obligation or by order of a regulatory authority

8. This certificate shall remain in full force and effect until the occurrence of the following event or the expiry of the following timeline, whichever is later

a. Completion of the project or termination of the contract (for any reason whatsoever), and fulfilment of all obligations relating to the return or secure destruction of information as specified in Clause 6; *and*
b. Execution of a subsequent agreement between the parties executed for the continuation or extension of the purpose covered under this certificate.

9. This certificate shall be governed by and constructed in accordance with the laws of India. Any dispute related to this certificate shall be subject to the exclusive jurisdiction of the Honorable High Court at Calcutta.

Anything found in contravention of the above, WBSEDCL may impose penalties, recover damages, blacklist the Vendor, or terminate the contract.

Signature with Office Seal

Annexure-X

PROFORMA OF "CONTRACT AGREEMENT"

(To be executed on non-Judicial stamp paper of Rs. 100/-)

This Agreement made this.....day of.....two thousand..... between West Bengal State Electricity Distribution Company Limited, having its head office at Vidyut Bhawan, Bidhannagar, Kolkata – 700 091 (hereinafter referred to as `Owner' or `WBSEDCL', which expression shall include its administrators, successors and assigns on one part) and **M/S ----------** ----------(hereinafter referred to as the `Contractor' , which expression shall include its administrators, successors, executors and permitted assigns) on the other part.

AND WHEREAS **M/S ----------** had awarded the Contract on terms and conditions, documents referred to therein, which have been acknowledged by **M/S ----------** resulting into a "Contract".

1) NOW THEREFORE THIS DEED WITNESSETH AS UNDER: -

1.0 **Article**

1.1 Award of Contract

WBSEDCL awarded the Contract to Contractor **for Implementation of SD-WAN, Managed Switch and Network Upgradation under offices of WBSEDCL** on the terms and conditions contained in its Letter of Award No. ----------. and the documents referred to therein. The award has taken effect retrospectively from the date of issue of the Award. The terms and expressions used in this Agreement shall have the same meaning as are assigned to them in the `Contract Documents' referred to in the succeeding Article.

2.0 Documentation

The Contract shall be performed strictly as per the terms and conditions stipulated herein and in the following documents attached herewith (hereinafter referred to as "Contract Documents").

i. LOA No. ----------

All the aforesaid Contract Documents shall form an integral part of this Agreement, in so far as the same or any part conform to the Bidding Documents and what has been specifically agreed to by the Owner in its Letter of Award. Any matter inconsistent therewith, contrary or repugnant thereto or any deviations taken by the Contractor in its `Proposal' but not agreed to specially by the Owner in its Letter of Award shall be deemed to have been withdrawn by the Contractor. For the sake of brevity, this agreement along with its aforesaid Contract Documents shall be referred to as the `Contract Agreement'.

3.0 Conditions & Covenants

3.1 The scope of Contract, Consideration, Terms of Payment, Taxes wherever applicable, Insurance, Liquidated Damage, SLA, Performance Guarantees, Technical Annexures, Other Annexure requirements and all other terms and conditions as contained in WBSEDCL's Letter of

Award No. ---------- shall be read in conjunction with Contract Documents. The Contract shall be duly performed following the Contract Documents.

3.2 The scope of work technical and functional requirements shall also include supply, delivery, installation, maintenance and other activities of all such items which are not specifically mentioned in the Contract Documents, but which are needed for successful, efficient, secure and reliable operation unless otherwise specifically excluded in the specifications under `exclusions', or `Letter of Award'.

3.3 The contract performance guarantee furnished by the Contractor is irrevocable and unconditional and the Owner shall have the powers to invoke it notwithstanding any dispute or difference between the owner and the contractor pending before any Court, Tribunal or any other authority.

3.4 This Agreement constitutes full and complete understanding between the parties and terms of the presents. Any modification of the Agreement shall be effected only by a written instrument signed by the authorized representative of both the parties.

4.0 SETTLEMENT OF DISPUTES

4.1 During execution of this contract, if any dispute arises thereby, shall be settled amicably between WBSEDCL and yourself to the extent possible**.**

4.2 The necessary legal affairs and / or court case shall be exclusively within the jurisdiction of Hon'ble High Court at Calcutta only.

4.3 Notice of Default: Notice of default given by either party to the other party under the Agreement shall be in writing and shall be deemed to have been duly and properly served upon the parties hereto if delivered against acknowledgement or by fax or by registered mail with acknowledgements due addressed to the signatories at the addresses mentioned at Kolkata.

IN WITNESS WHEREOF, the parties through their duly authorized representatives have executed these presents (execution whereof has been approved by the competent authorities of both the parties) on the day, month and year first above mentioned at Kolkata.

---------- **(Signature of Ordering Authority with Printed Name, Designation, Office Seal)**
---------- (**Signature of Contractor with Printed Name, Designation, Company's Seal)**

Annexure-XI

Mandatory Condition

Sl No.	Requisite Credential	Requisite Supporting document	Submitted Yes/No	Page Number
1	The bidder should be registered under the Companies Act, 1956 (substituted by Companies Act 2013) or a partnership firm or a firm of individual for more than 3 (three) years ending with 31.03.2022.	a) Certificate of incorporation as a Company under Companies Act. or a registered partnership deed or trade license as the case may be. b)Memorandum and Articles of Associations should be attached.		
2	**SDWAN Experience:** **The bidder** must have successfully implemented and/or managed a minimum of 750 SD-WAN devices of same OEM, in the last seven (7) years from date of publishing of tender in one or maximum of two LOA's. **For OEM** – successful installation and operation of a minimum of 1500 SD-WAN endpoints (hardware/software) in the last seven (7) years from the date of publishing of the tender, executed under one (1) or a maximum of two (2) Letters of Award (LOA). In addition, the OEM must have live and operational SD-WAN deployments as on the date of publishing of this tender, providing active support for a minimum of 500 SD-WAN boxes, over and above the above-mentioned deployments, executed under one (1) or maximum of two (2) Letters of Award (LOA).	Copies of the relevant Order(s).		
3	**Managed Switch Experience**: **The bidder** must have successfully implemented and/or managed a minimum of 800 managed switches in the last seven (7) years from date of publishing of tender in one or maximum of two LOA's. **For OEM** -minimum 1500 managed switches in the last seven (7) years from date of publishing of tender in one or maximum of two LOA's.	Copies of the relevant Order(s)..		

Sl No.	Requisite Credential	Requisite Supporting document	Submitted Yes/No	Page Number
	In addition, the OEM must have live and operational Managed switch deployments as on the date of publishing of this tender, providing active support for a minimum of 500 managed switches, over and above the above-mentioned deployments, executed under one (1) or maximum of two (2) Letters of Award (LOA).			
4	**Agent-Based Deployments Experience**: **For bidder** minimum 1000 client endpoints installation and management experience for NAC/AAA/EDR/any agent-based application etc in the last seven (7) years from date of publishing of tender in one or maximum of two LOA's. **For OEM** minimum 15,000 NAC/AAA agents, in the last seven (7) years from date of publishing of tender in one or maximum of two LOA's. In addition, the OEM must have live and operational NAC-AAA deployments as on the date of publishing of this tender, providing active support for a minimum of 1000 devices/users, over and above the above-mentioned deployments, executed under one (1) or maximum of two (2) Letters of Award (LOA).	Copies of the relevant Order(s).		
5	The bidder must possess a valid ISO 27001:2022 or latest certification.	Certificate copy of the same.		
6	The bidder must have one office in Kolkata, West Bengal for providing necessary support. If office already exists in Kolkata or The details of the office needs to be provided by the selected bidder prior to placement of the LOA (Letter of Award)/ contract.	a. Relevant Documents supporting the existence of an office in kolkata. b. Declaration signed by the Authorized Signatory to open an office in Kolkata prior to placement of the LOA (Letter of Award)/ contract.		
7	The bidder should not have been blacklisted from any Govt. organization across India in last three years.	An undertaking in this regard should be provided by the authorized signatory of the bidder.		

Sl No.	Requisite Credential	Requisite Supporting document	Submitted Yes/No	Page Number
8	The bidder should have a minimum annual turnover of INR 100 crore (Rupees One Hundred Crore only) in each of the last three financial years ending on 31.03.2025 (i.e., FY 2022–23, 2023–24, and 2024–25).	Provide the turnover in a separate sheet **(as <u>per Annexure-II</u>)** with Auditor's signature along with following supporting document duly attested i. Audited Balance Sheet and tax audit report for last 3 financial years ending with 31.03.2025 as applicable.		
9	Must Comply with all statutory obligations.	Provide the following required nos. in a separate sheet **(as <u>per Annexure-II</u>)** duly attested with following supporting documents. i. Copy of PAN Card ii. GST Certificate iii. Corporate Identification Number (CIN)		
10	GST return of 2023-24 and 2024-25	The bidder shall submit the relevant documents.		
11	The bidder should have a positive net worth in each of the last three financial years, i.e., FY 2022–23, 2023–24, and 2024–25.	Net worth certificate from any Chattered Firm.		
12	The bidder must submit a valid and original Manufacturer Authorization Form (MAF) from the respective OEM's for each and every hardware device, software component, controller, appliance, and solution proposed in this project.	OEM /OEM's MAF		
13	Common Criteria Certificate certified by a CCRA-recognized scheme or an Indian CCTL laboratory (STQC/MeitY) for SDWAN	Relevant Certificate		
14	Certificates related to cryptographic modules compliant with internationally recognized security standards—such as FIPS 140-2/140-3 (Level 2 or higher)/ any equivalent certification issued by an accredited IPv6 testing laboratory or Government of India–approved lab Undertaking by OEM, details in SDWAN technical Annexure.	Relevant Certificate/Undertaking		

Sl No.	Requisite Credential	Requisite Supporting document	Submitted Yes/No	Page Number
15	Certification IPv6 Ready Logo /any equivalent certification issued by an accredited IPv6 testing laboratory or Government of India–approved lab/undertaking by OEM, details in SDWAN technical Annexure.	Relevant Certificate/Undertaking		
16	Technical Annexures (Annexure T-1 to T-10) jointly signed and stamped by the Bidder/System Integrator and the respective OEM(s) for the products being supplied. Technical Annexures (Annexure T-11 to T-14) – To be signed and stamped by the Bidder/System Integrator.	Signed Document		

Signature of the bidder with Office Seal

Annexure-XII

Access Security Policy

(To be submitted on non-Judicial stamp paper of Rs. 100/-)

Access Security Policy
• User shall access only the appropriate physical area of the premises and appropriate information resource. • Users shall not access any information resources of WBSEDCL, without prior authorization of the concerned officials of WBSEDCL. • User shall not carry any Personal storage media like USB, Hard drives, DVD/CDs into secured zones like Data Centre, Disaster Recovery Centre, Vidyut Bhavan, etc. • Users shall not access any information resources without the presence of WBSEDCL's authorized personnel. • Any passwords and access privileges given shall not be disclosed to anyone inside and outside WBSEDCL's physical and logical boundaries. • Users shall not engage in abusive or improper use of information resources, which includes, but is not limited to, misuse of resource/ privileges, tampering with resource and unauthorized removal of resource components. • User shall not conduct or permit "hacker" activities. User shall not run "packet sniffers". Users shall not distribute computer viruses, Trojan horses, worms, or any other malicious software.
I hereby declare that I have understood the information security practices followed at WBSEDCL, and I shall adhere to the procedures.

Signature with Office Seal

Form - I

SCHEDULE OF BIDS

1	Name of the bidder with Registered office address Tel No. ,E-mail address	:		
2	Category of organization/company of the bidder with CIN Number	:		
3	Name of the Authorized Signatory for the Bid	:		
4	a) Earnest Money (Amount and in the form of BG/Online Payment) submitted:	:		
	b) In case EMD is submitted via BG, Branch Name of the Branch, Name of the Bank, Communication Address & IFSC code of the BG issuing bank	:		
5	Goods and Services Tax (GST) registration No.	:		
6	Professional Tax Registration Number	:		
7	Address of Kolkata office and Tel no/Fax no/E.mail address with the name of contact person	:		
8	Valid Trade License Number	:		
9	PAN Card No	:		
10	Offer valid upto	:	**180 days from the next date of opening of Tender.**	
11	The price should be Firm.	:	**The Prices are Firm.**	
12	If any deviation, please mention in deviation sheet enclosed (deviations mentioned elsewhere will not be considered)	:	**No Deviation**	

(Signature and Seal of Bidder)

Form - II

CHECK LIST

Bidders are required to upload the scan copy of all the documents, required as per tender specification and NIeT and verify before submission of Tender and also upload the Check list in the following format, duly digitally signed.

Sl. No.	Scanned Copy of Documents to be uploaded	Name of folder	To be submitted in cover	Submitted (Y/N)	Page Number
1	Earnest Money Deposit -Scanned copy BG (**Annexure -III**) if EMD paid through BG	**Drafts**	Statutory cover (Technical proposal)		
2	The **contact details** (communication address, mobile No. and email address) of the branch of the concerned Bank where the Bank Guarantee is issued	**Drafts**	Statutory cover (Technical proposal)		
3	Bid Proposal **(Annexure-I)**	**Annexures**	Statutory cover (Technical proposal)		
4	Price schedule in un-priced condition (**Annexure-VIII**).	**Annexures**	Statutory cover (Technical proposal)		
5	Bid Details **(Annexure-II)**	**Annexures**	Statutory cover (Technical proposal)		
6	Deviation Sheet **(Annexure-IV)**	**Annexures**	Statutory cover (Technical proposal)		
7	Blank Format of Proforma for bank guarantee for contract performance (**Annexure-V**)	**Annexures**	Statutory cover (Technical proposal)		
8	Contract Agreement (**Annexure-X**) - **On stamp paper during LOA placement, during tender on plain paper.**	**Annexures**	Statutory cover (Technical proposal)		
9	Non-Disclosure Agreement (**Annexure-IX**) and Access Security Policy **(Annexure- XII) -On stamp paper during LOA placement, during tender on plain paper.**	**Annexures**	Statutory cover (Technical proposal)		
10	Mandatory Condition (**Annexure-XI)**	**Annexures**	Statutory cover (Technical proposal)		
11	All technical Annexures **(T1 to T14)** signed by bidder and Technical Annexures relevant to OEM's	**Annexures**	Statutory cover (Technical proposal)		
12	Notice Inviting e-Tender	**NIT**	Statutory cover (Technical proposal)		
13	Addenda / corrigenda, if published	**NIT**	Statutory cover (Technical proposal)		
14	Schedule of bids duly filled in (**Form-I)**	**Forms**	Statutory cover (Technical proposal)		
15	Summary statement of annual turnover **(Form-III)**	**Forms**	Statutory cover (Technical proposal)		
16	Declaration of not being Blacklisted/Debarred/ Put on Holiday list **(Form-V)**	**Forms**	Statutory cover (Technical proposal)		
17	Self-declaration by Proprietor of the Bidding Company for not being Blacklisted/Debarred/ Put on Holiday list **(Form-VI)**	**Forms**	Statutory cover (Technical proposal)		
18	Declaration regarding no litigation against WBSEDCL **(Form-VII)**	**Forms**	Statutory cover (Technical proposal)		
19	Proforma for undertaking to be submitted by the Bidders **(Form-IV,VIII)**	**Forms**	Statutory cover (Technical proposal)		

Sl. No.	Scanned Copy of Documents to be uploaded	Name of folder	To be submitted in cover	Submitted (Y/N)	Page Number
20	Format of Letter of Bid **(Form-IX)**	**Forms**	Statutory cover (Technical proposal)		
21	Certificate of Incorporation indicating the CIN number	Company details	Non-statutory cover (Technical proposal)		
22	Copy of Valid copy of PAN Card	Certificates	Non-statutory cover (Technical proposal)		
23	Copy of IT Returns of last Three years are to be submitted by the Bidder i.e. for Financial years **2022-23, 2023-24 & 2024-25.**	Certificates	Non-statutory cover (Technical proposal)		
24	Copy of Valid Goods and Services Tax (GST) Registration certificate	Certificates	Non-statutory cover (Technical proposal)		
25	GST return for years **2023-24 & 2024-25**	Certificates	Non-statutory cover (Technical proposal)		
26	Copy of ISO: 270001 certificates (for Bidder)	Certificates	Non-statutory cover (Technical proposal)		
27	The bidder should have a minimum annual turnover of INR 100 crore (Rupees One Hundred Crore only) in each of the last three financial years ending on 31.03.2025 (i.e., FY 2022–23, 2023–24, and 2024–25).	Certificates	Non-statutory cover (Technical proposal)		
28	The bidder must have one office in Kolkata, West Bengal for providing necessary support. If office already exists in Kolkata or The details of the office needs to be provided by the selected bidder prior to placement of the LOA (Letter of Award)/ contract.	Credential	Non-statutory cover (Technical proposal)		
29	Bill of Quantities.	**BOQ**	Finance cover (Financial proposal)		

NOTE- The order and page numbering of the documents shall be **strictly followed** as mentioned above. In case any document is **not found, misplaced, or submitted out of sequence**, leading to failure in technical evaluation, the **sole responsibility shall lie with the bidder**.

NOTE- Bidders are strictly advised not to submit any documents other than those specifically requested in this RFP. Submission of additional or unsolicited documents may lead to processing difficulties, including jumbling or omission of required documents. Any extra documents submitted shall not be considered for evaluation and will not earn any additional credit.

(Signature and Seal of Bidder)

Form -III

Certificate regarding Summary Statement of Yearly Turn over

This is to certify that the following statement is the summary of the audit report /tax audit report arrived in favour of ..... for the three consecutive years or for such period since inception of the Firm, if it was set in less than such three year's period.

Sl. No.	Financial		Remarks
	Year	Turnover rounded up to two digits after decimal (Rs. In Lakh)	
1.	**2022-23**		
2.	**2023-24**		
3.	**2024-25**		
Total			

AverageTurnover:

Note:

Average turnover is to be expressed in lakh of rupees, rounded upto two digits after decimal.

(Signature and Seal of Bidder)

Form -IV

PROFORMA FOR UNDERTAKING TO BE SUBMITTED BY THE BIDDER

(For genuineness of the information furnished on-line and authenticity of the documents produced before Tender Committee for verification in support of his eligibility)

I ----------, Partner/Legal Attorney/ Accredited Representative of M/s ----------, solemnly declare that:

1. We are submitting Tender for the Work ---------- against Tender Notice No. ---------- dt. ----------
2. None of the Partners of our firm is relative of employee of ---------- (Name of the Company).
3. All information furnished by us in respect of fulfilment of eligibility criteria and qualification information of this Tender is complete, correct and true.
4. All documents/ credentials submitted along with this Tender are genuine, authentic, true and valid.
5. If any information and document submitted is found to be false/ incorrect any time, department may cancel my Tender and action as deemed fit may be taken against us, including termination of the contract, forfeiture of all dues including Earnest Money and banning / delisting of our firm and all partners of the firm etc.

(Signature and Seal of Bidder)

Dated----------

Form-V

(On the Bidder's Letterhead)

Declaration of not being Blacklisted/Debarred/ Put on Holiday list

Certified that our Company, M/s ……. is not blacklisted/debarred/suspended or put on Holiday list by any Statuary/ Regulatory/Government Authorities/ State Electricity Utility/ PSU in India.

It is certified that the information furnished above is true to the best of my knowledge and belief.

Bidder's Name:
Signature of the Tenderer:
Designation:
Seal of the Company:
Date:

Form-VI

(On the Bidder's Letterhead)

Self-declaration by Proprietor of the Bidding Company for not being Blacklisted/Debarred/ Put on Holiday list

I hereby confirm and declare that, none of the other concerns of which I am a proprietor / Managing Partner are blacklisted/ debarred/ suspended or put on holiday list by any Statutory/ Regulatory/ Government Authorities/ Sate Electricity Utility/ PSU in India.

It is certified that the information furnished above is true to the best of my knowledge and belief.

Signature of the Proprietor:
Name:
Designation:
Seal of the Company:
Date:

Form-VII

(On the Bidder's Letterhead)

Declaration regarding no litigation against WBSEDCL

We hereby declare that, no legal litigation/arbitration is pending/ongoing against WBSEDCL in any court/Forum against/by the bidder or its sister concern/Director/Partner/Proprietor.

If it is found at any stage of tendering, our offer will be rejected and I/We don't have any objection on the same.

Bidder's Name:
Signature of the Tenderer:
Designation:
Seal of the Company
Date:

Form-VIII

PROFORMA FOR UNDERTAKING TO BE-SUBMITTED BY THE BIDDER

(For genuineness of the information furnished on-line and authenticity of the document Produced before Tender Committee for verification in support of his eligibility)

I, ……,Partner/Legal Attorney/Accredited Representative of M/s ……., solemnly declare that:

1. We are submitting Tender for the Work ……. Against Tender Notice No. …….. dt…….
2. None of the Partners of our firm is relative of employee of …….. (Name of the Company)
3. All information furnished by us in respect of fulfilment of eligibility criteria and Qualification information of this Tender is complete, correct and true.
4. All documents/ credentials submitted along with this Tender are genuine, authentic, true and valid.
5. If any information and document submitted is found to be false/incorrect any time, department may cancel my Tender and action as deemed fit may be taken against us, including termination of the contract, forfeiture of all dues including Earnest Money and banning/delisting of our firm and all partners of the firm etc.

(Signature of Authorized Signatory)

Name:

Designation:

Seal:

FORM-IX

Format of Letter of Bid

LETTER HEAD OF BIDDER (AS ENROLLED ONLINE ON e-Tendering PORTAL OF NIC)

To

The Tender Committee

Sub: Letter of Bid for the work

……

……

……

……

Ref: 1. NIT No. …….. Dated ……..

2. Tender Id No. ……..

Dear Sir,

We offer to execute the work as per our offered bill of quantity in accordance with the conditions of the NIT document as available in the website. The details of the EMD being submitted by us has been furnished on-line.

This Bid and your subsequent Letter of Acceptance Work Order shall constitute a binding contract between us.

We hereby confirmed our acceptance of all the items and conditions ofthe NIT document unconditionally.

(Signature of Authorized Signatory)

Name:

Designation:

Seal: