



GUJARAT INFORMATICS LIMITED

Block No. 2, 2nd Floor, Karmayogi Bhavan,
Sector-10 A, Gandhinagar 382 010
Phone No: 079 - 23256022

**Bid for Design, Deployment, Integration,
Operation, and Maintenance of an SD-WAN
Overlay Solution over the existing GSWAN Hybrid
WAN Architecture across the State of Gujarat.
(Tender No. HWT05082026)**

Pre-Bid meeting: 12.08.2026 1500 hours

Last Date of Submission of Bid: 27.08.2026 till 1500 hours

Last Date of Submission of Bid Processing Fees & EMD: 27.08.2026 till 1500 hours

Bid Processing Fee: Rs.17,700/-

Introduction:

Gujarat Informatics Limited (GIL), on behalf of the DST (Department of Science and Technology), Govt. of Gujarat, Gandhinagar (herein after referred as the “TENDERER”) invites the bidders for Deployment, Integration, Operation and Maintenance of an SD-WAN Overlay Solution over the existing GSWAN Hybrid WAN Architecture across the State of Gujarat.

Bidder is requested to offer the cost for all the items, hardware, software, license and all the accessories as mentioned in bid document. GIL does not guarantee any fixed quantity at the time of signing the tender.

Proposals in the form of BID are requested for the item(s) in complete accordance with the documents to be uploaded as per the following guidelines:

- a. The bidder shall be required to submit a non-refundable Bid Processing Fee of ₹17,700/- (Rupees Seventeen Thousand Seven Hundred only) as specified in the bid document.
- b. Bidder shall submit their bids. The Bidder will have to submit the Earnest Money Deposit (E.M.D.) of **2 Crore Rs.** (Rupees Two Crore only) (Refundable) stipulated time defined in the bid in a sealed cover at GIL office with the heading “EMD for **Tender No HWT05082026** for rate contract for Deployment, Integration, Operation and Maintenance of an SD-WAN Overlay Solution over the existing GSWAN Hybrid WAN Architecture across the State of Gujarat.
- c. EMD as mentioned above, shall be submitted in the form of Demand Draft OR in the form of an unconditional Bank Guarantee (which should be valid up to validity of **9 months** from the date of bid submission) of any Nationalized Bank (operating in India having branch at Ahmedabad/ Gandhinagar) in the name of “Gujarat Informatics Ltd.” payable at Gandhinagar and must be submitted along with the covering letter.
- d. Please affix the stamp of your company on the overleaf of demand draft.
- e. Bidder has to submit Earnest Money Deposit in the form of Bank Guarantee as per below:
"All Nationalized Bank including the public sector bank or Private Sector Banks or Commercial Banks or Co-Operative & Rural Banks (operating in India having branch at Ahmedabad/ Gandhinagar) as per the G.R. No. FD/MSM/e-file/4/2024/2859/DMO dated 01/05/2025 issued by Finance Department or further instruction issued by Finance department time to time.
- f. In case of RTGS, please find below bank details of Gujarat Informatics Ltd
Saving Account No: 50200010918090
IFSC Code: HDFC0000190
Bank Name: HDFC
Bank Branch Address: Sector-16, Gandhinagar
 - 1) The bid shall specify time schedule of various activities.
 - 2) Bid complete in all respects should be uploaded on or before the Bid due date.
 - 3) Interested and eligible Bidders are required to upload the eligibility related document in Eligibility Bid Section, technical related document in Technical Bid Section & commercial bid in Commercial Bid Section. The Bids should be accompanied by a bid security as specified in this Bid Document. The Eligibility, Technical & Commercial Bid must be uploaded & the Bid Security must be delivered to the office of Gujarat Informatics Ltd.
 - 4) Bidders are required to mention Make and Model of the product.
 - 5) Product and Services offered should be strictly as per requirements mentioned in this Bid document. No deviation shall be accepted under any circumstances.
 - 6) Once quoted, the bidder shall not make any price changes, whether resulting or arising out of any technical/commercial clarifications sought regarding the bid. Such price changes shall render the bid liable for rejection.
- g. Performance Bank Guarantee (PBG)

The Successful Bidder shall furnish a Performance Bank Guarantee (PBG) to DST/GIL for an amount equivalent to 5% of the total value of the Order/LOI towards faithful performance of the contract obligations and satisfactory performance of the services during the contract period.

The Performance Bank Guarantee shall be submitted within 15 working days from the date of issuance of the Work Order/Letter of Intent (LOI).

The PBG shall:

- Be denominated in Indian Rupees.
- Be in the form of an unconditional Bank Guarantee.
- Be issued by any Nationalized Bank / Public Sector Bank / Private Sector Bank / Commercial Bank / Co-operative Bank / Rural Bank operating in India having a branch at Ahmedabad or Gandhinagar.
- Be valid for a period up to 180 days beyond the completion of the Contract period.

The PBG shall be submitted as per the format prescribed by DST/GIL, attached as an Annexure to this RFP, and in accordance with the Finance Department G.R. No. FD/MSM/e-file/4/2024/2859/DMO dated 01/05/2025, or any subsequent instructions issued by the Finance Department from time to time.

In case of breach or non-compliance of contractual obligations, SLA terms, or other conditions of the contract, DST/GIL shall have the right to invoke the Performance Bank Guarantee.

The Performance Bank Guarantee shall be released and returned to the Successful Bidder within 30 days after the expiry of its validity, subject to satisfactory completion of all contractual obligations.

- h. In case of non-receipt of Bid Processing fees & EMD as mentioned above within prescribed time, the bid will be rejected by GIL as non-responsive.
- i. Unsuccessful/Disqualified bidder's E.M.D. will be returned as promptly as possible but not later than 15 days after the expiration of the period of bid validity OR upon the successful Bidder signing the Contract, and furnishing the Performance Bank Guarantee @ 5% of the total order value as prescribed, whichever is earlier.
- j. In exceptional circumstances, GIL may solicit the Bidder's consent to an extension of the period of validity. The request and the responses thereto shall be made in writing. A Bidder may refuse the request without forfeiting its E.M.D. A Bidder granting the request will not be permitted to modify its bid.
- k. The Successful bidder has to submit copy of acceptance of purchase order & copy of PBG.

SECTION 1

KEY INFORMATION

Key Information:

Gujarat Informatics Limited (hereinafter referred to as “GIL”), on behalf of Department of Science & Technology (hereinafter referred to as “DST”), Govt. of Gujarat (hereinafter referred to as “Tenderer”) intend to invite offers for Bid for Design, Deployment, Integration, Operation, and Maintenance of an SD-WAN Overlay Solution over the existing GSWAN Hybrid WAN Architecture across the State of Gujarat.

1	Contact Person	Shri. Maulik Chauhan, GM (Tech & Network) Gujarat Informatics Ltd gm-tech@gujarat.gov.in Phone no. : 079-232 59238 Shri. Prakash Dholakia, GM (Networking) Gujarat Informatics Ltd dgmTech-gil@gujarat.gov.in Phone no. : 079-232 52026 Jitendra Chauhan, Manager (Networking) Gujarat Informatics Ltd srmgr1-gswan@gujarat.gov.in Phone no. : 079-232 58155
---	----------------	--

Pre-bid Meeting:

The pre-bid queries/clarifications, if any, should be submitted in writing to Gujarat Informatics Limited by end of the day of the pre-bid meeting date. Thereafter, the clarifications received from the bidders will not be entertained.

Pre-Bid meeting: 12.08.2026 1500 hours

Please address all pre-bid queries and correspondence to

1. Shri Prakash Dholakia, GM (Networking), Gujarat Informatics Limited, Block No. 2, 2nd Floor, Karmayogi Bhavan, Sector-10A, Gandhinagar 382010, Phone No. 079-23252026.
2. E-mail: Gm-tech@gujarat.gov.in; DgmTech-gil@gujarat.gov.in; Srmgr1-gswan@gujarat.gov.in

Project Objectives:

The primary objective of this project is to implement a robust, secure, scalable, and centrally managed SD-WAN overlay solution across GSWAN, capable of: - Seamless connectivity between State Headquarters (SHQ), State Data Centre (SDC), District Centers (DC), Taluka Centers (TC), Point-of-Presence (PoP) locations, and horizontal offices - Operating over a hybrid underlay network consisting of MPLS, Internet, ILL, P2P, and wireless links - Supporting multiple network topologies including Hub-and-Spoke, and Full Mesh - Providing intelligent traffic steering, application-aware routing, and integrated security.

The solution shall optimize network traffic between remote office locations and SHQ/SDC using suitable mechanisms to ensure efficient utilization of available bandwidth. It shall support load distribution across multiple active paths and automated failover to maintain service continuity and enhance link performance.

The SD-WAN solution shall include an integrated **Quality of Service (QoS)** framework with application-level awareness, bandwidth prioritization, and dynamic path selection capabilities. This includes routing latency-sensitive application traffic through the most optimal path or, where applicable, splitting application traffic across multiple paths to improve overall performance.

Key Features Required in the SD-WAN Solution

The proposed SD-WAN solution must include, but not be limited to, the following features:

1. Zero-touch provisioning (ZTP)
2. Application-aware routing
3. Bandwidth aggregation
4. Centralized Network performance parameters, Network outage, Device Outage, policy-driven dashboard
5. Application-wise QoS
6. LAN traffic segmentation
7. Dynamic WAN traffic load balancing (application-based)
8. Application-wise bandwidth utilization and analytics
9. Automated outage detection and correction
10. Real Time Monitoring of Network Performance metrics (latency, packet loss, jitter) and traffic forwarding to optimal Path
11. The SD-WAN solution deployed at hub and branch locations shall support integrated security capabilities such as Intrusion Prevention System (IPS), anti-malware protection, botnet detection and prevention, application control, and malicious URL/web filtering, DoS protection available from the initial deployment.
12. The solution should support Secure Web Gateway capabilities and provide policy-based control for web and application access, including the ability to monitor and restrict unauthorized data sharing or file uploads.

SECTION 2

ELIGIBILITY CRITERIA

SECTION 2

Eligibility Criteria:

Sr. No.	Parameters	Attachments
1.	Bidder should be IT/ITeS Company registered under Indian Companies Act 1956/2013,	Certificates of incorporation & Self-Declaration Certificates
2.	The bidder should have successfully supplied and implemented SD-WAN / WAN / MPLS / Hybrid WAN solutions in State Government Organizations / Central Government / PSU / Listed Companies / BFSI during the last five (5) years, as per any one of the following criteria: a) One (1) project covering 4,800 or more locations, or b) Two (2) projects, each covering 3,000 or more locations, or c) Three (3) projects, each covering 2,400 or more locations. The locations shall be distinct operational sites connected under a single managed WAN/SD-WAN architecture.	Details of such projects undertaken along with work order/purchase order copy/clients' completion certification/letter signed/ e-mail issued by authorized signatory or company secretary with the details w.r.t to the clause should be enclosed.
3.	The bidder must have average annual turnover of Rs. 200 Crore (Minimum) in the last three financial years as on 31st March 2025.	The copies of Audited Annual Accounts/Balance Sheet along with Profit & Loss Account and CA Certified Statement with UDIN for last three financial years as on 31st March 2025 shall be attached along with the bid.
4.	The OEM & bidder must have positive Net worth or should be Profit making in any three financial years out of last four Financial Year as on 31st March 2025.	The copies of CA Certified Statement for last three financial years as on 31st March 2025 shall be attached along with the bid.
5.	The quoted products of OEM should have an average annual related turnover of not less than Rs 500 Crores in last three years FY-22-2023, 23-2024, 24-2025.	The copies of Audited Annual Accounts/Balance Sheet along with Profit & Loss Account and CA Certified Statement with UDIN for last three financial years as on 31st March 2025 shall be attached along with the bid.
6.	The OEM of proposed product must have supplied SD-WAN edge device/Secure SD-WAN appliance with minimum quantity of 15,000 in State Government Organizations / Central Government / PSU / Listed Companies / BFSI during the last five (5) years before the bid opening date.	Details of such projects undertaken along with work order/purchase order copy/clients' on-going or completion certification/letter signed/ e-mail issued by authorized signatory or company secretary with the details w.r.t to the clause should be enclosed.

Sr. No.	Parameters	Attachments
7.	The bidder must have one office in Gujarat.	Please upload the copies of any two of the following: Property Tax Bill of last year / Electricity Bills of last one year / Telephone Bills of last one year / G.S.T. Registration / Valid Lease Agreement. In case, bidder does not have office in Gujarat, bidder should give undertaking to open office in Gujarat within 45 days from the date of purchase order.
8.	Bidder and OEM should not be blacklisted/debarred by any state government / central government / PSU in last three years as on last date of bid submission.	Bidder and OEM will have to submit undertaking letter at the time of bidding
9.	The Bidder and OEM should have a Customer Support Center which operates 24x7x365 and is capable of troubleshooting 24x7x365 days	A Self Certified letter with Address
10.	The quoted product must be MTCTE certified.	MTCTE certification
11.	The OEM shall comply with the Government of India guidelines regarding restrictions on procurement from bidders/OEMs of countries sharing land borders with India, as applicable and amended from time to time. Necessary declarations and supporting documents, if required, shall be submitted in accordance with the applicable Government of India orders	Required document with authorized signatory

Note:

- Bidder will have to submit Self-Declaration letter for acceptance of ATC Given in bid.**
- OEM will have to submit undertaking letter by mentioning that manufacturing of the quoted items manufactured in current Year.**
- The Bidder must attach valid documents in support to their Technical and Financial capabilities/strength, as mentioned above. Without proper supporting documents, the Bid proposals are liable to be rejected.**
- Consortium is not allowed.**
- The OEM shall submit an undertaking/acceptance confirming compliance with the SD-WAN key features and functional requirements, on the OEM's official letterhead, duly signed and stamped by the authorized signatory.**

SECTION 3

Scope of Work

3.1 Scope Overview

The Successful Bidder and OEM shall be responsible for the **design, supply, installation, configuration, integration, testing, operation, and maintenance** of the SD-WAN overlay solution in accordance with this RFP.

3.2 Overlay vs Underlay Responsibility

- a) The SD-WAN solution shall function strictly as an overlay network over the existing GSWAN underlay connectivity.
- b) The OEM shall be responsible for designing the complete overlay and underlay network architecture required for the proposed SD-WAN solution across all locations. The design shall include selection and sizing of appropriate transport technologies such as P2P links, L2/L3 MPLS, ILL, Broadband, and wireless connectivity options including 3G/4G/LTE/5G, ensuring optimal performance, redundancy, high availability, and scalability for the SD-WAN overlay.
- c) The OEM shall provide detailed underlay design recommendations including bandwidth sizing, link redundancy model, routing architecture, failover mechanisms, QoS considerations, and integration with the SD-WAN overlay policies.
- d) However, the actual provisioning, commissioning, and maintenance of the underlay circuits shall be carried out separately by telecom / network service providers appointed by DST/GIL. The bidder shall coordinate with such service providers to ensure proper integration, configuration compatibility, and end-to-end functionality of the SD-WAN solution.
- e) SLA accountability of the Bidder shall be limited strictly to SD-WAN overlay components only.

3.3 Key Responsibilities of the Bidder

The Successful Bidder and OEM shall: - Design and deploy an on-premises SD-WAN architecture - Ensure active-active utilization of multiple WAN links - Integrate centralized orchestration, monitoring, analytics, and security - Coordinate with GSWAN Operations Teams - Provide documentation, training, and OEM support.

The Successful Bidder shall be solely responsible for the complete design, supply, installation, integration, testing, commissioning, migration, implementation, operation, maintenance, warranty, OEM support, training, documentation, and successful functioning of the proposed SD-WAN solution in accordance with this RFP.

The Bidder shall provide all hardware, software, firmware, licenses, subscriptions, accessories, transceivers, passive components, cables, connectors, racks, mounting accessories, tools, utilities, documentation, professional services, OEM services, manpower, security components, integration services, third-party interfaces, testing equipment, consumables, and any other item or service required for successful implementation and operation of the complete solution, irrespective of whether specifically mentioned in the RFP.

Any item, activity, software, hardware, license, service, or component reasonably required for achieving the intended functionality, performance, interoperability, security, scalability, availability, compliance, or successful operation of the solution shall be deemed to be included in the Bidder's scope and quoted price. No additional payment, change request, variation order, or financial claim shall be admissible on account of omission, oversight, misunderstanding, or interpretation of the RFP.

3.4 Functional Requirement

1. The Bidder is required to submit a detailed proposed solution, including the topology and an implementation plan with timelines aligned to those mentioned in the RFP.
2. SD-WAN Orchestrator and Controllers shall be deployed on premise within Government Data Centre / designated location. Public cloud-only orchestration shall not be acceptable.
3. The SD-WAN Central Orchestrator shall be deployed in High Availability mode across Primary Data Centre and Disaster Recovery Data Centre with automated database replication, policy synchronization and controller failover. There shall be no single point of failure in the management infrastructure.
4. The Successful Bidder shall plan and design the network in such a way that devices utilize multiple links actively for load balancing and for the functioning of other SD-WAN features in the network
5. The solution should be capable of utilizing a combination of two or more links in any of the following scenarios:
 - a) Point-to-Point links, L2 MPLS, L3 MPLS, Internet Leased Line, 3G/4G/5G/LTE, Broadband Internet, etc.

6. The Successful Bidder is required to engage skilled resources necessary for the successful completion of the project within the stipulated timelines specified in the RFP.
7. The Bidder is required to coordinate with GSWAN's existing Operations Team and the GSDC Operations Team throughout the tenure of the contract.
8. The SD-WAN solution provided by the Successful Bidder should be horizontally scalable to support additional connectivity expansion.
9. The bidder is required to design, supply, and provision hardware, software, and licenses for the SD-WAN core infrastructure capable of supporting a minimum of 6,000 SD-WAN devices/sites with minimum two link termination at each location from Day-1 of commissioning. The solution must also support an additional 30% scalability (1,800 devices), making the total capacity 7,800 devices, without any augmentation or upgrade of hardware, software, or licenses. The bidder should ensure that this scalability is built-in within the proposed architecture, and no additional cost should be payable by the Department for enabling or utilizing this additional capacity during the contract period.
10. The proposed Central Orchestrator infrastructure shall support minimum 7,800 SD-WAN Edge devices, associated tunnels, policies and analytics from Day-1 without any hardware or software augmentation.
11. In the event that the proposed devices resource utilization goes high, the device should not go in bypass mode and should continue to process the traffic without service disruption with all policies configured and enabled. The product should not have SLA impact with all the functionalities as prescribed in RFP at any time during the contract period. The bidder will have to replace device with higher capacity resource at no cost to DST / GIL at any time during the contract period. The bidder will have to replace device with higher capacity resources at no cost to DST/GIL at any time during the contract period.
12. The SD-WAN OEM shall provide professional services for the design, validation, and initial implementation of the SD-WAN solution. The OEM shall be responsible for designing, validating, and implementing the SD-WAN Controller and SD-WAN Hub at the State Headquarters (SHQ). Further, as part of OEM professional services, the OEM shall directly design and implement a minimum 100 sites to establish the reference architecture, validate performance, and ensure correct deployment standards. Thereafter, the remaining site implementations may be carried out by the Bidder under the guidance, validation, and certification of the OEM.
13. The SD-WAN solution must be implemented in such a way that incoming and outgoing traffic is automatically load-balanced across network links at branches, even when the primary link is not fully utilized. Traffic should be distributed across network links even when the links are not congested.
14. The SD-WAN solution should support export of device configurations for audit purposes and restoration as needed.
15. All components of the proposed SD-WAN solution must be **on-premises**.
16. The Hub and Branch CPE Appliance should have the Hardware/virtual appliance. In case of virtual appliance all required hardware, software, license etc. shall be provided by the bidder as part of the solution.
17. All transceivers shall be sourced from the same OEM or and shall be fully compatible with the proposed device. Necessary fiber patch cords shall also be provided as per site requirements.
18. The proposed SD-WAN solution should support Hub & Spoke, Partial Mesh, network topologies from Day 1. During the implementation spoke to spoke connection between all the branches should be achieved with either dynamic or static full mesh.
19. The proposed SD WAN solution component should be IPv6 ready logo or USGv6 certified. Must support IPv4 and IPv6 protocols from day 1.
20. The proposed SD-WAN branch appliance shall be quoted with maximum supported license tier by the hardware platform. The appliance should meet the requirements specified in the RFP while also supporting future scalability without hardware replacement.
21. The proposed SD-WAN solution should provide a dashboard for monitoring all links and appliances. It should also support link utilization, availability, SLA reporting, packet loss, and latency reporting.
22. The dashboard shall provide graphical topology, WAN path visualization, application analytics, SLA compliance, tunnel health, alarms, security events and historical trend analysis
23. The proposed solution must be able to monitor and report top applications by usage across all links. It must identify and report at least the top 20 applications based on ports and IP addresses. The application signature updates should have a frequency weekly.
24. In the proposed SD-WAN solution, administrators should be able to drill down into reports for troubleshooting (e.g., applications accessed by a specific host along with bandwidth consumed within a defined timeframe).
25. The proposed SD-WAN solution should support management through CLI and Web GUI interfaces.
26. The proposed SD-WAN solution must support partial software upgrades, allowing the network administrator to selectively upgrade software at specific sites without upgrading all sites simultaneously.
27. The Successful Bidder must provide equipment meeting the functional requirement and specifications mentioned under Section-5.

28. The Successful Bidder will be responsible for integrating Log Analysis and Reporting solutions with the existing solution of GSWAN/GSDC (NMS/SIEM/SOAR).
29. The Successful Bidder should provide onsite resources for the implementation, commissioning and operation and maintenance of the devices. If any major SD-WAN–related issue arises during implementation and post Go-live of the project that impacts GSWAN operations and the Bidder fails to rectify it within **24 hours**, the Bidder must involve OEM Technical Experts/TAC Support/TAC on Site support until permanent resolution is achieved. Status updates must be shared with DST/GIL, and an RCA report must be submitted.
30. If any device or component becomes faulty, the Successful Bidder shall replace it as per the SOW and SLA defined in the RFP. The Bidder must also install a standby device of similar make/model or equivalent (from the same OEM), ensuring the network remains functional within the defined SLA. The standby device must not be EOS. In case of RMA, the Bidder must replace the equipment as per SLA and return the faulty equipment to the OEM warehouse at no extra cost to DST/GIL. The Bidder must maintain sufficient inventory to meet SLA requirements.
31. All modules, licenses, power cables, and sub-components should be bundled or mapped with the parent device, and their warranty/AMC should be **co-terminous** with the parent device.
32. The Successful Bidder shall promptly address and remediate all audit observations, compliance issues, and VA/PT findings at no additional cost to DST/GIL. All identified vulnerabilities shall be remediated based on their severity and exploitability in accordance with industry standards (such as CVSS or equivalent). Critical and High severity vulnerabilities, particularly those that are actively exploitable, shall be remediated on priority and within the shortest possible timeframe, without dependency on mutually agreed timelines. In the event that a General Availability (GA) patch or stable fix has not yet been released by the OEM, the OEM shall provide an interim fix, hotfix, or appropriate mitigation mechanism to address the vulnerability. The Bidder shall ensure immediate deployment of such interim fix or mitigation to minimize security risk. Once the official GA patch or permanent fix is released by the OEM, the Bidder shall ensure its deployment at the earliest to achieve full compliance.
33. The new devices supplied by the Bidder shall become DST/GIL assets. The Bidder shall maintain adequate stock of spare equipment or components to meet SLA uptime requirements.
34. The Successful Bidder should provide login credentials to DST/GIL/GSWAN Operation team to access the OEM portal for call logging, support, and viewing the status of calls/TAC cases raised for GSWAN.
35. Whenever an issue is reported by GSWAN Team, the Successful Bidder shall troubleshoot it in a time-bound manner in coordination with GSWAN Team and simultaneously log a ticket with OEM TAC.
36. Tenderer should be able to log support calls **24x7 via phone/email/web-portal** directly with the OEM without dependency on the Successful Bidder.
37. The Tenderer shall have administrator-level access to the Central Orchestrator throughout the contract period, including configuration backup, policy management, monitoring, reporting and audit logs.
38. The Successful Bidder must remove all cables from the existing equipment and terminate them on the new SD-WAN equipment. All uplinks and cables must be reconnected neatly (including rack dressing).
39. The Successful Bidder must appoint and depute a dedicated resource for device deployment and support services, who will act as a **Single Point of Contact (SPOC)** for the entire project.
40. The Successful Bidder must ensure migration of existing equipment configurations to the new SD-WAN equipment with **Near Zero downtime**.
41. The Successful Bidder must provide network logical and physical topology diagrams, IP addressing, routing and switching strategy, equipment datasheets, configuration guides (GUI/CLI), configuration files/templates/policies, SOP documents, and other documentation as per industry standards or DST/GIL requirements.
42. The Successful Bidder shall arrange training and certification on the SD-WAN solution from the OEM for officers nominated by DST/GIL. Training documentation must be prepared and shared to DST/GIL.
43. The Successful Bidder must provide issue-based categorization (hardware/software), troubleshooting manuals, and RCA documentation with recommended remedies.
44. Any additional hardware or accessories required for successful implementation and compliance with the RFP requirements, though not explicitly mentioned, shall be provided by the bidder at no additional cost. No extra claims shall be admissible.
45. All SD-WAN device, software, routing, security, security signature updates, orchestration, analytics, subscription services and management licenses shall be perpetual or subscription (with 10 years license to be supplied from day 1) in nature from the Go-Live of the project. No feature reduction, throttling, or license expiry shall occur after completion of the mentioned period.
46. The TAC support for both hardware and software should be provide by the same SDWAN OEM.
47. BIDDER and OEM must have Dedicated/toll free Telephone No. for service support.
48. The bidders should submit the escalation matrix for delivery & installation and for support services (contact persons details & e-mail ids). The escalation matrix should have separate support engineer and project manager under this project.

49. All security and networking features specified in the RFP shall be supported natively on the SD-WAN solution or through tightly integrated OEM-supported components/companies without requiring additional third-party products.
50. The solution shall support standard IPsec-based interoperability for underlay connectivity and shall not restrict migration or coexistence with future WAN technologies.
51. The solution shall support quantum-resistant cryptography and incorporate AI/ML-based capabilities for predictive analytics, proactive monitoring, trend analysis, automated troubleshooting, and orchestration-driven predictive diagnostics.
52. The proposed solution shall support centralized logging and shall store all logs in compliance with the policies and guidelines issued by Department of Telecommunications, Telecom Regulatory Authority of India, and Indian Computer Emergency Response Team for the specified retention period as mandated from time to time.
53. The solution shall comply with all applicable CERT-In, DoT, and TRAI guidelines, including, but not limited to, log retention and secure maintenance of records. The successful bidder shall implement all necessary measures to ensure compliance as part of the solution including all network device configuration files shall be securely backed up within India, version-controlled, encrypted, and retained for a minimum of 2 years, ensuring availability for audit, recovery, and compliance verification. Bidder has to provide the necessary logs whenever asked by GIL / competent authority. Bidder should deploy any tool / solution for ip address management / syslog to ensure necessary compliance and retention for 2 years as asked above.
54. Configuration backups of the Central Orchestrator shall be encrypted, version controlled and replicated between DC and DR with automated scheduled backup.
55. The Successful Bidder shall be solely responsible for delivering and ensuring the complete solution as per the requirements specified in the RFP. In order to achieve the intended solution, the bidder shall provide any additional hardware, software, licenses, accessories, active/passive components, and all related services, if required. All such provisions shall be deemed to be included in the bid price, and no additional cost shall be payable by the tenderer.
56. Upon delivery of materials at the designated Central Locations or the Vendor's Warehouse at Gandhinagar/Ahmedabad, the Successful Bidder shall formally intimate and offer the items for inspection to the Purchaser. DST/GIL or its authorized agency shall inspect the supplied components to verify compliance with RFP specifications and BoM. The bidder shall provide necessary support and documentation. Any defects or non-compliance observed shall be rectified or replaced by the bidder within the stipulated timeline at no additional cost.
57. No End-of-Life (EoL) or End-of-Support (EoS) product shall be quoted in the bid. The make and model proposed by the bidder shall remain available and supported by the OEM for the entire contract period, including availability of spares, patches, and technical support. All supplied components shall be new, unused, and of the latest manufacturing year. If OEM declares EOS/EOL during contract bidder shall replace with equivalent or higher model without additional cost.
58. The Successful Bidder shall be fully responsible for end-to-end deployment, installation, integration, and commissioning of the SD-WAN solution at the Disaster Recovery (DR) site location as identified and confirmed by DST/GIL within country, without any additional cost to the Purchaser.
59. The Bidder shall ensure seamless integration and synchronization between Primary (DC) and Disaster Recovery (DR) locations, including configuration replication, policy synchronization, and centralized management through the SD-WAN controller/orchestrator. The solution shall support automated and consistent policy enforcement across DC and DR environments.
60. The Bidder shall configure and demonstrate automated and/or manual failover and failback mechanisms between DC and DR locations. In the event of failure of the Primary (DC) site, traffic shall be seamlessly redirected to the DR site with minimal disruption. The solution shall support automated failover within 30 seconds and manual failover within 5 minutes.
61. SDWAN solution should have packet level / policy level insight with the graphical representation ability to generate the synthetic traffic probes to check any and analyze the traffic flow.
62. The SDWAN Solution must provide advanced network visibility and diagnostic that includes packet level flow, policy level insight across the fabric the platform should offer graphical representation of traffic paths and behavior and must include the ability to generate synthetic traffic proactively verify application experience and WAN performance.
63. The bidder shall ensure that all proposed hardware, software, operating systems, firmware, and solution components comply with the security requirements and policies of Gujarat State Data Centre (GSDC). The bidder shall undertake all activities required for security compliance, security hardening, Vulnerability Assessment and Penetration Testing (VAPT), remediation of identified vulnerabilities, and obtain all necessary approvals/certifications required by GSDC for deployment and operation. All such activities shall be carried out by

the bidder without any additional cost to the Tender Inviting Authority throughout the implementation, warranty, and contract period without any additional cost to the Tender Inviting Authority.

3.5 Design Principles to be followed

- a. **Minimal manual intervention** during operations to reduce dependency on technical manpower deployed at sites.
- b. **Security policies** must be configured for all devices and controllers to prevent unwanted intrusions, including IPS, Malicious URL filtering, and detection of known and unknown malware.
- c. The solution must provide **in-depth traffic analysis** to detect and prevent malicious traffic and internal threats through system-generated alerts.
- d. **Automated prioritization of traffic** should be supported based on DST/GIL requirements (e.g., prioritizing WAN traffic for critical GSWAN applications over non-critical traffic).
- e. Traffic and traffic policies must be **centrally managed and controlled**, with configurations pushed from the central controller/manager.
- f. The solution should support **automated traffic diversion based on link performance**. Traffic should be diverted to stable paths based on defined thresholds and restored automatically once the impacted link stabilizes.
- g. The solution must support **alert notifications via email, SMS, or WhatsApp** upon crossing system or user-defined thresholds.
- h. The solution shall ensure centralized policy administration with complete audit logging and rollback capability for all configuration changes.

3.6 Operating Conditions

- a. **Reliability:** The proposed solution must support 24x7x365 round-the-clock operations.
- b. **Upgradeability:** The system should be modular, easily reconfigurable, and upgradeable.
- c. **Completion of Contract:** At the time of contract completion, all devices must be handed over with complete documentation, including configurations, integration details, and troubleshooting manuals. All devices should be fully functional and covered under valid support.
- d. **Security:** As GSWAN is the backbone network for Government departments, the solution must be fully secure with best-in-class security features. Minimum required features include:
 1. Solution must be part of the SD-WAN fabric.
 2. Application visibility, reporting, filtering, and policy enforcement.
 3. URL filtering support.
 4. Security rules must be easy to deploy, manage, update, and enforce universally.
 5. Reporting capabilities either on-device or via third-party/API integration.
 6. The centralized SD-WAN management platform shall support logical segregation of networks or administrative domains (e.g., organization/department level separation) along with role-based access control (RBAC) to enable controlled access and management privileges for different users or administrative groups.

3.7 Guidelines for Installation and Commissioning

1. Perform all general tests, including physical checks at delivery, pre-installation verification, ensuring correct implementation and connections, and confirming completeness of system documentation.
2. The Successful Bidder shall comply with all **safety regulations and practices**.
3. The Successful Bidder shall perform all tests in accordance with SD-WAN specifications mentioned in the technical compliance section and the design principles defined in the Scope of Work.
4. The Successful Bidder shall provide **on-site warranty** for all components (hardware, software, etc.) for a period of **five years** and for any extended period of contract from the date of the Final Acceptance Test completion certificate. Warranty, post-warranty maintenance, and spare-parts support must cover all hardware, software, accessories, cabling, and required AMC for the entire contract duration.

3.8 Manpower Deployment, Knowledge Transfer & Handover

Background: DST/GIL has GSWAN established centralized operations team responsible for statewide WAN monitoring, incident logging, coordination, and first-level support.

The successful bidder shall provide specialized SD-WAN manpower to support stabilization, knowledge transfer, and transition of operations to the GSWAN Operations Team.

A. Scope & Duration of Manpower Deployment:

1. The bidder shall deploy the required SD-WAN manpower **only for a period of one (1) year post Go-Live.**
2. The objective of manpower deployment shall be:
 - a) Stabilization of the SD-WAN solution
 - b) Advanced troubleshooting and root cause analysis
 - c) Configuration and policy support
 - d) Knowledge transfer and operational handover to GSWAN operation team
3. Post completion of the one-year period, **no dedicated manpower deployment by the bidder shall be mandatory**, except for obligations under SLA, warranty, OEM support, or AMC.

B. Minimum Manpower Requirement:

Role	Minimum Count	Key Responsibilities
SD-WAN L3 / Solution Architect	1	Architecture oversight, policy design, RCA, upgrades
SD-WAN L2 Engineer	1	Configuration support, fault isolation, coordination
SD-WAN Orchestrator / NMS Specialist	1	Monitoring, analytics, reporting, NMS integration
Service Delivery Manager	1	SLA tracking, reporting, coordination with GSWAN & TPA

C. Responsibilities & Coordination:

1. The bidder's manpower shall work in **close coordination** with the GSWAN Operations Team.
2. GSWAN Operations Team shall continue to handle:
 - a) First-level monitoring
 - b) Incident logging
 - c) Initial coordination
3. The bidder shall be responsible for:
 - a) L2/L3 support
 - b) Advanced troubleshooting
 - c) SD-WAN platform configuration
 - d) OEM escalation and coordination

D. Onsite / Field Support

1. The bidder shall provide **on-call field support** for:
 - a) P1 and P2 incidents

- b) Hardware replacement
- c) Critical rollout or configuration activities

E. Knowledge Transfer (KT) & Handover

1. The bidder shall conduct **structured knowledge transfer sessions** covering:

- a) SD-WAN architecture and design
- b) Policy and configuration management
- c) Monitoring and reporting
- d) Incident and problem management
- e) Upgrade, rollback, procedures

2. The bidder shall submit:

- a) As-built documents
- b) SOPs and operational run books
- c) Administrator-level access credentials

3. Successful completion of KT and handover shall be:

- a) Certified by DST/GIL

F. Handover Completion

Upon completion of one (1) year post Go-Live, the bidder shall formally hand over SD-WAN operations to GSWAN and demonstrate operational readiness of the GSWAN team.

DST/GIL shall issue a **Handover Completion Certificate** upon satisfactory completion.

G. Continuity & Replacement

1. The bidder shall ensure continuity of services during the manpower deployment period.
2. In case of attrition, the bidder shall replace the concerned resource within **7 calendar days**, without impact on SLA or services.
3. For any absence or non-availability of a deployed manpower resource, a penalty of ₹1,000 (Rupees One Thousand only) per absent resource per calendar day shall be applicable from the first day of absence / absconding until the resource resumes duty or a replacement resource is deployed. The bidder shall ensure continuity of services at all times, and such absence shall not affect the delivery of services under the Contract. Penalty shall be levied from the quarterly payment milestone M5 of payment schedule.

3.9 Final Acceptance Testing (FAT) & Go-Live

1. Acceptance Testing shall be carried out for each site/location in accordance with the scope, requirements, specifications, and design principles defined in this RFP.
2. Acceptance testing for each location shall be conducted by the empaneled Third Party Agency (TPA) of GSWAN, in coordination with the tenderer.

3. The Successful Bidder shall submit a detailed Acceptance Testing Plan (ATP) prior to FAT, covering test methodology, test cases, SD-WAN features, performance parameters, redundancy, security features, and applicable SLA parameters.
4. The Successful Bidder shall demonstrate and document all functionalities, features, configurations, and integrations relevant to this project to the satisfaction of the tenderer and its designated agency.
5. Availability of all defined services shall be verified during FAT by the tenderer and its designated agency. The bidder shall demonstrate all features, facilities, and functionalities as specified in this RFP.
6. The Final Acceptance Certificate (FAC) shall be issued by the tenderer and its designated agency upon successful completion of FAT for the Hub / Central Location.
7. The date of issuance of the Final Acceptance Certificate for the Hub / Central Location shall be deemed the “Go-Live” date, after which the project shall enter the Operation and Maintenance (O&M) phase, and applicable SLAs shall come into effect.
8. Following are the minimum test case to be check during the FAT. However, DST/GIL or its designated agency reserves the right to verify full compliance with the RFP requirements. The Successful Bidder shall be required to successfully complete all test cases and demonstrate compliance as part of the FAT.

Sr. No.	Test Category	Test Case	Test Description	Expected Result
1	ZTP	Zero Touch Provisioning	Device auto registers and downloads configuration	Device commissioned without manual intervention
2	Overlay	Tunnel Establishment	Establish IPSec tunnels across multiple WAN links	Secure overlay tunnels established successfully
3	Routing	Application Aware Routing	Verify application-based path selection	Traffic follows configured SLA and policy
4	Failover	WAN Link Failure	Primary WAN link failure	Traffic switches within OEM committed convergence time (maximum 800 ms)
5	Load Balancing	Active-Active WAN	Traffic distribution across multiple WAN links	Load shared as per policy
6	Performance	Throughput Test	Measure SD-WAN throughput with security enabled	Meets committed throughput
7	High Availability	Edge Device HA	Primary appliance failure	Secondary appliance assumes operation without session interruption
8	Security	Firewall & Security Policies	Verify firewall, IPS, URL filtering, AV, App Control policies	Policies enforced successfully
9	Segmentation	VRF/Zone Segmentation	Verify network segmentation	No traffic leakage between segments
10	QoS	Application Prioritization	Voice, Video and Business Applications	QoS policy applied correctly
11	Video	Real-Time Traffic	Voice & Video conference	No noticeable packet loss, jitter or latency degradation
12	Monitoring	Dashboard Verification	Real-time monitoring and topology	Correct status displayed
13	Logging	Syslog Integration	Forward logs to Syslog/SIEM	Logs received and searchable

14	Backup	Edge Configuration Backup	Backup and restore edge configuration	Configuration restored successfully
15	Resilience	Headless Operation	Disconnect Controller	Edge devices continue forwarding using last synchronized policy
16	Controller HA	Controller Node Failure	Shutdown one controller node	No management interruption
17	Controller DR	DC-DR Failover	Fail primary controller site	Automatic failover and synchronization
18	Policy Management	Bulk Policy Push	Deploy policy to multiple devices	Policy successfully deployed
19	Configuration	Rollback	Rollback configuration	Previous configuration restored
20	Backup	Controller Backup & Restore	Restore Controller database	Successful recovery
21	RBAC	Role Validation	Validate user permissions	Role-based access enforced
22	Software Upgrade	Phased Upgrade	Upgrade selected devices	Upgrade completed without service disruption
23	Audit	Audit Trail	Verify administrator actions	All actions logged
24	Certificate	Certificate Renewal	Renew certificates	Tunnel remains operational
25	Routing	OSPF/BGP	Verify dynamic routing	Routes exchanged correctly
26	Routing	Static Routing	Verify static route operation	Traffic forwarded correctly
27	VPN	IPSec Interoperability	Establish VPN with third-party device (if applicable)	Tunnel established successfully
28	SLA	Latency, Jitter & Packet Loss	Validate SLA monitoring	Values reported correctly
29	Analytics	Application Visibility	Generate application reports	Reports generated successfully
30	API	Northbound API	Verify REST API integration	API responds correctly
31	SNMP	NMS Integration	Verify SNMP monitoring	Device monitored successfully
32	Alerts	Alarm Notification	Generate threshold alarm	Email/SNMP Trap/Webhook generated
33	Licensing	License Validation	Verify all subscribed features	All licensed features operational
34	Scalability	Multiple Edge Registration	Register multiple edge devices simultaneously	Controller provisions all devices successfully
35	Template	Template Deployment	Deploy configuration templates	Templates applied successfully
36	Reporting	Historical Reports	Generate utilization/SLA reports	Reports exported successfully

37	Controller Performance	Concurrent Operations	Simultaneous monitoring, policy deployment and reporting	No performance degradation
38	Security	Administrator Authentication	LDAP/AD/RADIUS/TACACS+ login	Authentication successful
39	Management	Configuration Version Control	Multiple configuration revisions	Version history maintained and rollback available
40	Interoperability	Existing NMS/SIEM Integration	Verify integration with existing GSWAN tools	Successful event and log exchange

3.10 Delivery Milestone:

Milestone	Deliverable	Timeline	Penalty
1	Submission of Performance Bank Guarantee (PBG) and conduct of Project Kick-off Meeting	T + 15 calendar days	In case of non-submission of PBG within the specified timeline, the Earnest Money Deposit (EMD) shall be forfeited , and the tenderer reserves the right to cancel the award.
2	Delivery of all components (Hardware, Software, Licenses, etc.) at Central Locations / Vendor Warehouse at Gandhinagar / Ahmedabad	T1 = T + 45 calendar days	A penalty of 0.15% per week or part thereof of the Total Contract Value (TCV) shall be levied for delays beyond specified timeline, subject to a maximum of 20% of the TCV .
3	Installation, and Commissioning of SD-WAN solution at Hub / Central Locations	T2 = T1 + 60 calendar days	A penalty of 0.15% per week or part thereof of the Total Contract Value (TCV) shall be levied for delays beyond specified timeline, subject to a maximum of 20% of the TCV .
4	Final Acceptance Testing (FAT) of the SD-WAN solution at Hub / Central Locations	T3 = T2 + 15 calendar days	A penalty of 0.15% per week or part thereof of the TCV shall be levied for delays beyond specified timeline, subject to a maximum of 20% of the TCV .
5	Installation, Commissioning, and FAT of SD-WAN Edge Devices at Individual Office Locations	T4 = T1 + 90 calendar days	A penalty of 0.15% per week or part thereof per delayed site/location shall be levied for delays beyond the specified timeline, subject to an overall maximum of 20% of the TCV .
6	Installation, and Commissioning of SD-WAN solution at District Locations, Taluka and PoP Locations	T5 = T1 + 100 calendar days	A penalty of 0.15% per week or part thereof of the Total Contract Value (TCV) shall be levied for delays beyond specified timeline, subject to a maximum of 20% of the TCV .
7	Final Acceptance Testing (FAT) and Go-Live of the SD-WAN solution for District, Taluka and PoP Locations	T6 = T5 + 15 calendar days	A penalty of 0.15% per week or part thereof of the TCV shall be levied for delays beyond specified timeline, subject to a maximum of 20% of the TCV .

1. T = Date of issuance of Contract
2. In case, the selected bidder does not supply the ordered items for any reason, the bidder will be liable to pay the difference amount to the purchaser, over and above the performance guarantee.
3. The above delivery-related penalties are independent of and in addition to the Service Level Agreement (SLA) penalties applicable during the Operation & Maintenance phase.

4. Installation, commissioning, and FAT of Edge devices shall be carried out on a site-wise basis provided the Edge devices are operational and integrated with the Core infrastructure.
5. Edge deployment shall be executed, accepted, and (if applicable) paid on a pro-rata basis linked to the number of sites successfully commissioned and FAT completed.

SECTION 4

Service Level Agreement, Penalties & Payment Terms

SECTION 4

Service Level Agreement, Penalty, and Payment Terms applicable within Contract and Warranty Period.

5.1. Scope and Applicability

These Operational SLAs shall be applicable for the SD-WAN overlay solution deployed under the GSWAN / State Wide Area Network, including SD-WAN CPE, overlay network, centralized controllers, hubs, and network management systems. The scope of these SLAs expressly excludes underlay / last-mile network connectivity, which is managed separately by an existing service provider appointed by DST/GIL. The Bidder shall be responsible only for SLA compliance of the SD-WAN overlay components defined herein.

5.2. Network Availability SLA (for SD-WAN Overlay)

Sr. No	Network Element	SLA Requirement
1	State Data Centre (SDC) / Hub Availability/SD-WAN Controller/Central Infrastructure	≥ 99.99%
2	District Availability	≥ 99.99%
3	Taluka / PoP / Customer_Edge Site Availability	≥ 99.50%

5.3. Incident Response and Resolution SLA

Severity Level	Description	Response Time	Resolution Time
P1 – Critical	Site/Device outage, severe degradation of network performance KPIs (Automatic Link Failover, latency, jitter, packet loss, application availability, SD-WAN overlay functionality, controller availability, etc.) affecting Gandhinagar Secretariat, State Data Centre (DC), Disaster Recovery (DR), District/Taluka core infrastructure, or causing State-wide impact. Any Critical Security Incident affecting the confidentiality, integrity, or availability of the SD-WAN infrastructure at DC/DR/TC/ locations, including malware/ransomware infection, unauthorized access, controller compromise, VPN/certificate compromise, security policy breach, DDoS attack impacting SD-WAN services, lateral movement attempts, or any cyber incident requiring immediate containment.	≤ 15 minutes	≤ 1 hours
P2 – Major	Site/Device outage or severe performance degradation affecting a District offices and DC PoP without State-wide impact. Any Critical Security Incident affecting the confidentiality, integrity, or availability of the SD-WAN infrastructure at edge location of DC/TC/PoP locations, including malware/ransomware infection, unauthorized access, controller compromise, VPN/certificate compromise, security policy breach, DDoS attack impacting SD-WAN services, lateral movement attempts, or any cyber incident requiring immediate containment.	≤ 30 minutes	≤ 3 hours
P3 – Minor	Site/Device outage or severe performance degradation affecting a Taluka offices and TC PoP without State-wide impact.	≤ 2 hours	≤ 6 hours
P4 – Low	Configuration changes, information requests	≤ 24 Hours	≤ 48 Hours

5.4. SD-WAN Failover and Redundancy SLA measurement method

Parameter	SLA Requirement
Automatic Link Failover	Mandatory
Failover Time	Failover time of 300–800 ms shall be measured at SD-WAN overlay tunnel and live application level, without TCP/UDP session reset or user-visible disruption
Traffic Steering	Based on latency, jitter, and packet loss policies, BW utilization, etc.

5.5. SLA-wise Penalty Mapping (Overlay SLAs Only)

Sr. No.	SLA Parameter	SLA Requirement	Measurement & Applicability	Penalty Calculation	Maximum Penalty
1	State Data Centre (SDC) / Hub Availability/SD-WAN Controller/Central Infrastructure	≥ 99.99% per quarter	Availability shall be measured per site/location and aggregated quarterly across all central infrastructure sites.	A single quarterly penalty of 1% of QCV for every 0.1 percentage point shortfall of aggregated achieved availability below the SLA target. No per-site penalty shall be applied.	Up to 10% of QCV per quarter
1	SD-WAN Central Infrastructure Availability at DC locations	≥ 99.99% per quarter	Availability shall be measured per site/location and aggregated quarterly across all central infrastructure sites.	A single quarterly penalty of 1% of QCV for every 0.1 percentage point shortfall of aggregated achieved availability below the SLA target. No per-site penalty shall be applied.	Up to 10% of QCV per quarter
2	SD-WAN Edge Device Availability at TC/PoP/Customer Locations	≥ 99.70% per quarter	Availability shall be based on complaints logged by the office location through GSWAN helpdesk or SD-WAN monitoring system. Only complaint-based downtime is counted. Unreported downtime is excluded. Aggregated quarterly across all edge sites.	A single quarterly penalty of 1% of QCV for every 0.05 percentage point shortfall of aggregated achieved availability below the SLA target. No per-site penalty shall be applied.	Up to 5% of QCV per quarter
3	P1 Incident Resolution Time	≤ 1 hours	Measured per incident, per site/location	2% of QCV per incident breach, aggregated quarterly	Up to 10% of QCV per quarter

4	P2 Incident Resolution Time	≤ 3 hours	Measured per incident, per site/location	1% of QCV per incident breach, aggregated quarterly	Up to 5% of QCV per quarter
5	P3 Incident Resolution Time	≤ 6 hours	Measured per incident, per site/location	1% of QCV per incident breach, aggregated quarterly	Up to 5% of QCV per quarter
6	P4 Incident Resolution Time	≤ 2 business days	Measured per incident, per site/location	0.5% of QCV per incident breach, aggregated quarterly	Up to 5% of QCV per quarter
7	Non-submission of Monthly SLA Report	As specified in RFP	Measured per instance	0.5% of QCV per instance, aggregated quarterly	Up to 2% of QCV per quarter

Note:

- Penalties shall be applicable only to SD-WAN overlay components within the scope of this RFP.
- SD-WAN Edge Device Availability at Customer Locations SLA is only applicable to downtime periods reported via complaint through the official GSWAN helpdesk or SD-WAN monitoring.
- Availability for Central Infrastructure and Customer Edge Devices shall be computed on an aggregated basis across all applicable locations. No per-site penalty shall be levied.
- Penalties for underlay / connectivity-related failures shall not be applicable to the Bidder.
- The cumulative penalty in a quarter shall be capped at 25% of the quarterly contract value.
- Shortfalls are aggregated quarterly across all sites to calculate penalty.
- Penalties are applied once per quarter, not per site.
- Sites meeting SLA do not dilute the penalty for non-compliant sites.
- Rounding Rule: Fractional shortfalls are rounded up to the next penalty step.
- Total SLA penalties (availability + incident penalties) are capped at the overall maximum per quarter (e.g., 25% of QCV)

5.6. Sample: SLA Availability Penalty Calculation

5.6.1 Availability (%) per site

Formula:

$$\text{Availability (\%)} = ((\text{Total Time} - \text{Downtime} / \text{Total Time}) \times 100$$

5.6.2 Aggregated Achieved Availability (%)

Formula:

$$\text{Aggregated Achieved Availability (\%)} = (\sum \text{Availability of all non-compliant sites}) / (\text{Number of non-compliant sites})$$

5.6.3 Availability Shortfall (%)

Formula:

$$\text{Availability Shortfall (\%)} = \text{SLA Target (X\%)} - \text{Aggregated Achieved Availability (\%)}$$

5.6.4 Penalty Steps

Formula:

$$\text{Penalty Steps} = \text{CEILING}(\text{Availability Shortfall} / \text{Penalty Step (S\%)})$$

5.6.5 Availability Penalty (% of QCV)

Formula:

$$\text{Availability Penalty (\%)} = \text{Penalty Steps} \times \text{Penalty Rate (R\%)}$$

5.6.6 Final Availability Penalty (% of QCV)

Formula:

Final Availability Penalty (%) = min(Availability Penalty, Maximum Cap (M%))

5.6.7 Availability Penalty Amount

Formula:

Availability Penalty Amount = Final Availability Penalty (%) × QCV

Key Variables

- Total Time: Contracted service time window
- Downtime (complaint-based): Time service was unavailable
- SLA Target (X%): Minimum agreed availability threshold
- Penalty Step (S%): Increment threshold for penalties
- Penalty Rate (R%): Rate applied per penalty step
- Maximum Cap (M%): Maximum penalty limit
- QCV: Quarterly Contract Value (or agreed contract value basis)

5.7. SERVICE LEVEL AGREEMENT (SLA) & MEASUREMENT FRAMEWORK

A. SLA Measurement – System of Record

1. All SLA parameters including **availability, downtime, incident occurrence, incident resolution time, SLA compliance, and penalty calculation** shall be **measured, recorded, and reported exclusively** through the following authorized systems:
 - **GSWAN Helpdesk System**, and/or
 - **GSWAN Network Monitoring System (NMS)**, and/or
 - **Authorized SD-WAN Monitoring / Orchestration System integrated with GSWAN NMS.**
2. Any SLA data, reports, or calculations generated outside the above systems shall **not be considered valid** for SLA measurement or penalty computation.
3. The successful bidder shall ensure **seamless integration** of the SD-WAN monitoring/orchestration system with the GSWAN NMS

B. Incident Management & Measurement

1. All incidents shall be **logged, tracked, and closed** through the **GSWAN Helpdesk System**.
2. The **incident start time, acknowledgement time, resolution time, and closure time** recorded in the GSWAN Helpdesk System shall be treated as **final and binding** for SLA measurement.
3. Incident priorities (**P1 / P2 / P3 / P4**) as classified in the GSWAN Helpdesk shall be used for SLA compliance and penalty determination.

C. Availability Measurement Methodology

SD-WAN Central Infrastructure Availability (SDC / DC / TC / PoP)

1. Availability shall be measured using **GSWAN NMS and/or SD-WAN monitoring system**.
2. Availability shall be calculated **quarterly**, aggregated across all Central Infrastructure components.
3. Penalty shall be calculated based on **aggregated achieved availability**, not on individual device or site-wise penalties.

SD-WAN Edge Device Availability at Customer Locations

1. Availability of SD-WAN Edge Devices shall be measured on a **complaint-based model**.
2. Only downtime corresponding to **valid complaints logged by the respective office location in the GSWAN Helpdesk**, and corroborated by monitoring system logs, shall be considered for SLA calculation.
3. Downtime due to factors such as:
 - Power unavailability,
 - Office closure,
 - Device being switched off intentionally,
 - Any unreported outage
 shall **not be considered** unless a complaint is logged in the GSWAN Helpdesk.
4. Availability shall be **aggregated quarterly** across all non-compliant sites.
No per-site monetary penalty shall be applied.

5.8. SLA Exclusions

Sr. No.	Exclusion
1	Downtime attributable to underlay / last-mile connectivity provided by an existing service provider
2	Power failure due to DISCOM
3	Force majeure events
4	Planned maintenance approved by DST/GIL

5.9. Penalty and Termination

Parameter	Condition
Quarterly SLA Penalty Cap	25% of quarterly contract value
Chronic SLA Failure	Penalty exceeding 25% for two consecutive quarters

Action	Contract termination and forfeiture of PBG, at the discretion of DST/GIL
--------	--

5.10. SD-WAN Overlay Accountability

The Bidder shall be responsible for meeting the defined SLAs for the SD-WAN overlay solution only, including SD-WAN CPE, centralized controllers, orchestration, policy enforcement, monitoring, and integration with the existing GSWAN underlay network. The Bidder shall coordinate with the underlay connectivity service provider for fault isolation and resolution; however, SLA accountability for underlay connectivity shall remain outside the scope of this RFP.

5.11. TPA Measurement Methodology

The Third Party Auditor (TPA) shall measure SLA compliance based on data sourced from the centralized SD-WAN Network Management System (NMS), controller logs, and ticketing systems. SLA measurements shall consider only SD-WAN overlay components within the scope of this RFP.

5.12. Measurement Principles:

- Overlay availability shall be measured based on reachability of SD-WAN CPE to controllers.
- Performance metrics shall be derived from active and passive probes at the SD-WAN overlay level.
- Underlay connectivity downtime, when supported by documentary evidence and RCA, shall be excluded from SLA computation.
- Ticket timestamps recorded in the SD-WAN ticketing system / existing NMS of bidder shall be the basis for response and resolution SLA measurement.

5.13. Alignment with GSWAN / Hybrid MPLS–Internet Architecture

Component	GSWAN Alignment
Underlay Network	Existing P2P/L2/L3 MPLS / ILL / Broadband / 3G/4G/LTE/5G managed by DST/GIL-appointed vendor
Overlay Network	SD-WAN overlay with centralized orchestration
Traffic Steering	The dynamic path selection rules should allow traffic steering based on following parameters: ➤ Source IP address ➤ Source MAC address ➤ User identity and user groups (where identity integration is available) ➤ Destination IP address, route attributes/tags, and Type of Service (ToS) / DSCP values ➤ Application identification, application groups, or application categories ➤ Protocol type and QoS markings ➤ Link quality parameters or service level agreement (SLA) metrics such as latency, jitter, packet loss, or other defined performance thresholds.
Application Prioritization	Policy-based (VC, IP Telephony, critical apps)
High Availability	Dual hubs at SDC
Scalability	Support for district, taluka, and remote offices

The SD-WAN solution shall seamlessly integrate with the existing GSWAN underlay network and support hybrid MPLS, Internet, P2P, Broadband operations without disruption to existing services.

5.14. Payment Schedule:

Category	Milestone	Milestone Description	Payment
(Core SD-WAN Infrastructure, DC,TC,PoP & Customer Edge Locations)	M1	Delivery of all components (Hardware, Software, Licenses, etc.) at Central Locations / Vendor Warehouse at Gandhinagar / Ahmedabad	30% of total Contract Value Payment under M1 shall be released only after successful inspection of the material.
	M2	Final Acceptance Testing (FAT) of the SD-WAN solution at Hub / Central Locations	20% of total Contract Value
	M3	Installation, Commissioning, and FAT of SD-WAN Edge Devices at Office Locations (site-wise)	20% of total Contract Value (Pro-rata based on sites completed)

	M4	Final Acceptance Testing (FAT) of the SD-WAN solution for District, Taluka and PoP Locations.	20% of total Contract Value
	M5	Deployment of SD-WAN SI Manpower and provision of stabilization, knowledge transfer, operational support, and handover services for one (1) year from Go-Live	10% of the Total Contract Value, payable in four (4) equal quarterly instalments (2.5% each), subject to successful deployment of the required manpower, satisfactory service delivery, submission of quarterly reports, and compliance with the applicable SLA. Any applicable SLA penalties and manpower penalty shall be deducted from the respective quarterly payment.

General Payment & Billing Conditions

1. Payments shall be made **at the end of each quarter**, subject to acceptance of invoices by the **TPA or DST/GIL's designated agency**.
2. **Invoice Submission**
The bidder shall submit its **payment claim at the end of each quarter** through invoices, along with all relevant supporting documents and SLA reports
3. **Supporting Documentation**
any additional documents required in support of service performance, as deemed acceptable by the **Government of Gujarat (GoG)**, shall also be submitted by the bidder.
4. **Penalty and Tax Deductions**
DST/GIL shall be entitled to **deduct applicable SLA penalties at source** while making payments to the bidder. DST/GIL shall also deduct **TDS and any other applicable statutory taxes** at source, as amended from time to time.
5. Completion of knowledge transfer and formal handover to the GSWAN Operations Team is a mandatory prerequisite for release of the final quarterly manpower payment.
6. In case of delay, manpower support shall continue at no additional cost until successful handover.
7. Go-Live of the SD-WAN solution shall be declared only upon successful completion of all applicable FAT activities, including Core, District, Taluka, and PoP locations, along with the Edge locations (site-wise/batch-wise), and upon formal certification by the tenderer or its designated agency.
8. Warranty shall start from the Go-Live of the SD-WAN Solution.
9. Release of payments under Milestones M2, M3, and M4 shall be subject to successful completion of respective FAT activities. However, final project acceptance shall be governed by the Go-Live declaration as defined above. No claim of full project completion shall be considered until Go-Live is formally certified by the tenderer.
10. The first quarterly payment under Milestone M5 shall become due upon successful deployment of all approved manpower and completion of the first quarter of services from the Go-Live date. Subsequent quarterly payments shall be released after completion of each quarter, subject to certification by DST/GIL or its designated agency regarding satisfactory service delivery, compliance with the manpower deployment requirements, submission of all deliverables, and achievement of the applicable SLA.
11. In case any deployed manpower remains absent or vacant beyond the permissible replacement period specified in the RFP, the corresponding applicable penalties shall be deducted from the quarterly payment.

SECTION 5

SPECIFICATIONS

Section – 5

SPECIFICATIONS

5.1. SD-WAN – FUNCTIONAL – REQUIREMENT

Sr. No	Technical Requirement	Compliance (Yes/No)
1	All components of the proposed SD -Wan solution components must deploy On-premises.	
2	The proposed Secure SD WAN Solution should be implemented as true software-defined network architecture, SD-WAN network architecture should have a clear separation of required planes physically or logically. All Component of the solution should be on premise.	
3	The SD-WAN solution should have multi-WAN underlay support (P2P/L2/L3 MPLS / ILL / Broadband / 3G/4G/LTE/5G etc), multiple active-active Overlay tunnel support.	
4	The Secure SD-WAN solution should support Static routing, interior gateway protocols (iBGP, OSPF v2/v3 , RIPv1/V2 etc), Exterior Gateway Protocol (eBGP), VRF or equivalent, MP-BGP.	
5	The solution should offer flexible architectures including hub and spoke architecture along with partial mesh. Eg : District to all talukas below the district and district to district.	
6	The solution should support IPv4 and IPv6 dual stack from day one. The proposed solution and hardware should be IPv6 Ready logo and FIPS 140-2 or higher.	
7	The solution should support the following QoS features.	
	Classification	
	DSCP and TOS Marking	

	Policing	
	Scheduling	
	Shaping via various parameters - bandwidth limits per application, based on Percentage value etc.	
	Differentiated Services (DiffServ) and queuing mechanism based on interface/Policy	
8	SD-WAN Solution must be implemented in such a way that the traffic will be load balanced across wan links.	
9	The solution should be able to apply QoS based on the application.	
10	Should perform enhanced SD-WAN monitoring for each SD-WAN link with visibility of link status, application/link performance, and bandwidth utilization. The SLA targets or SD-WAN tunnel endpoints should be included in performance monitoring graphs for each WAN provider.	
11	The solution should support SNMPv3 and NTP	
12	The solution should offer flexible architectures: Hub-to-Spoke (partial mesh), Multi-Hub, Multi-Region, & Direct Internet Access / Remote Internet Access for the branches	
13	Solution should have Intelligent WAN path control and ability to direct traffic among WAN links based on the actual applications (L7) by configuring Granular Application policies and Application SLA based path selection. Should support active/active and active/standby path forwarding.	
14	The solution should recover from link failure - alternate link convergence time without session disconnect and No service interruption	
15	The solution should support Mean Opinion Score (MOS) or equivalent based SLA tracking for Voice and Video Traffic. In case the Voice/Video traffic crosses the threshold, it should automatically fall back to the other link.	
16	The proposed solution shall support comprehensive Network Address Translation (NAT) capabilities, including Static NAT, Dynamic NAT, Port Address Translation (PAT/NAT Overload), Source NAT (SNAT), Destination NAT (DNAT), Policy-Based NAT, NAT Exemption, and NAT46/NAT64 translation. The solution shall also provide comprehensive IPv6 networking support, including but not limited to IPv6-based management, IPv6 routing, IPv6 tunneling mechanisms, IPv6-based traffic steering within SD-WAN policies, IPv6-aware firewall policies, IPv6 IPsec VPN, and application visibility and control for IPv6 traffic.	
17	The devices should have a console / Management port	
18	The solution should support advanced path conditioning techniques like Packet duplication and forward error correction (FEC) to support uninterrupted, zero packet-loss transmission of real-time critical traffic.	
19	The solution must support Certificate management. Solution to support all versions SSL/TLS Inspection for inspection of invalid, expired, untrusted certificates.	
21	The solution should have the capability to measure application transactions (SLAs) such as latency, jitter, and packet-loss with built-in automatic fail-over to determine preferred paths and maintain the optimal application performance of business-critical applications.	
22	The solution should support extension of L2 network across sites over the SD-WAN fabric. It should also support MP-BGP EVPN with VXLAN.	
23	Bidirectional Forwarding Detection (BFD) features should be supported	
24	The solution should support Dynamic Forward Error Correction (FEC) for packet loss compensation on the overlay / underlay .	
25	The branch devices must be able to identify and recover from a transit link failure within 300-800 ms.	
26	The solution should support IP and User-based SD-WAN security policies. The solution shall support integration with NAC/AAA/identity platforms (e.g.,	

	AD/LDAP) for user authentication and maintenance of user-to-IP address mappings. The NAC/identity system shall be responsible for: • Authenticating users and endpoints • Maintaining user-to-IP correlation • Providing logs and visibility for security monitoring, auditing, and threat investigation	
27	The solution should be able to define and identify Custom applications based on IP address, port numbers or FQDNs. This information should be used to successfully perform SD-WAN steering of Custom HTTPS application traffic.	
28	The data traffic from branch sites must not be impacted in case of failure to reach any of the controllers/Manager (headless situation). Data paths must be maintained for at least 5 days without reachability to the central management system (controller, orchestrator).	
29	The solution should have secure TPM CHIPS for securely storing cryptographic keys. It should support encryption standards AES , DES, ESP and DH group.	
30	The proposed SD-WAN solution must support the following security capabilities at all locations.	
	Zone base protection	
	DDOS protection	
	L7 Firewall	
	Application based control	
	Anti Malware Protection	
	Malicious URL Filter	
31	IPS Protections	
	Signature and Updates:	
	Automatic signature update	
	Option to download these signatures from the Vendor's site manually and upload it to the Central Management / Orchestrator / Controller	
	Automatically download by the Central Management / Orchestrator / Controller from the Vendor's Update server and should support proxy connection	
32	shall automatically updated from the Central Management / Orchestrator / Controller to all Hub and Branch devices.	
	The proposed solution must support IP and User and User group-aware SD-WAN policies to prioritize traffic of VIP users, Ministers, and higher officials at any site.	
33	The proposed solution must be able to prioritize voice and data traffic using best practice methodologies like MOS / Quality Score to ensure effectiveness.	
34	SD-WAN solution should support all advanced SD-WAN features without any restriction, more than 1000 VRF, unlimited topologies, Per Packet / Session base Load balancing, Advanced QoS, FEC, Bandwidth Detection, Packet Duplication, Per Packet/Session base Steering, Unlimited topologies.	
35	All Hub devices /solutions (Central infrastructure including software and license and accessories) should be in HA with N+N set up with all SD-WAN features mentioned in this RFP at DC & DR location.	
Remote User Security and Access Management		
36	The proposed solution shall support secure remote access for users connecting from outside the enterprise network, enabling secure connectivity to both internet resources and enterprise/private applications through centralized policy enforcement.	

37	The solution should support remote user connectivity through a unified client/agent with centralized policy management, enabling consistent access control and security policies for users accessing enterprise applications and internet services. The solution should also support security inspection of remote user traffic as mentioned in this RFP	
Management, Monitoring and Reporting		
38	The Centralized Management / Orchestrator / Controller/Analytical platform can be Physical appliance OR Virtual Appliance OR Software Based should be from same OEM to be deployed on premise. In case of a software & Virtual option, the OS and hardware needs to be bundled along.	
39	The central management system should authenticate and authorize every administrator/user accessing the Central/branch device. The central management system should support integrations with AD, LDAP, radius, 2FA (2 Factor Authentication) using email/SMS.	
40	The solution must be capable of exporting traffic logs to external syslog servers & SIEM tool	
41	Should perform enhanced monitoring for each SD-WAN link member with visibility of link status, application performance, and bandwidth utilization. The SLA targets should be included in performance monitoring graphs for each WAN provider.	
42	The solution must be capable of sending alerts via email, SMS or Whatsapp on meeting/exceeding the user-defined thresholds.	
43	The solution must support a configuration rollback feature to detect and recover from software and configuration errors by reverting to previous active software or configuration	
44	The proposed SD-WAN solution shall provide advanced analytics and reporting capabilities for network and security monitoring. The platform should support visibility into bandwidth utilization, link performance metrics such as latency, jitter, and packet loss, real-time monitoring, and time-based filtering of reports. The solution should also provide WAN link SLA performance reports, application-level usage statistics, and security event visibility including threat intelligence details such as malware indicators, malicious domains or URLs, affected hosts and indicators of compromise (IOC).	
45	It should have a various view which provides centralized monitoring and awareness of the link outages, threats, events and network activity, with predefined / customized dashboards.	
46	Solution should be able to parse, correlate logs and generate reports for all the appliance supplied along with this solution.	
47	Provide various report on-demand or on a schedule with automated email in HTML / PDF / image format to a list of users. Solution should have various templets available to generate pre-defined reports also built-in report templates must be customizable	
48	The solution should support API-based integration.	
49	Should have Drill-down capabilities to follow the trail of sessions , trace transactions, and gain new insights and log search capabilities based on Usernames/ IP, service, Applications etc	
50	Should have Automated alert notification for issues, problems and attacks	
51	The system must be able to monitor ISP link parameters like link quality, link usage, and link congestion. It should be able to provide historical data on the same for a period as defined in Cert-In guidelines.	
52	Should have built-in report templates, which are customizable and shall have the facility to create custom reports.	
Compliance		
53	The proposed solution shall use cryptographic modules certified under FIPS 140-2 Level 2 or higher,	

54	The proposed solution shall be Common Criteria (CC) certified against the relevant Network Device Protection Profiles (NDPP). The Common Criteria certification shall be issued either by an internationally recognized Common Criteria Certification Scheme or by the Indian Common Criteria Certification Scheme (IC3S), established by the Ministry of Electronics and Information Technology (MeitY). Valid Common Criteria certification details shall be submitted along with the technical bid.	
55	The proposed solution components or its Operating System should be IPv6 logo and USGv6 certified	

5.2. SD-WAN SPECIFICATION:

SD-WAN General Specification:

The proposed SD-WAN Customer Premises Equipment (CPE) shall be a standards-based integrated device capable of functioning as a full-featured IP router in addition to SD-WAN overlay services. No separate router or additional network appliance shall be required to meet the routing, segmentation, VPN, QoS, or traffic engineering including but not limited to minimum requirements specified herein,

Category	Requirement
Device Type	SD-WAN Customer Premises Equipment (CPE) with integrated, full-featured IP router and security functionality. No separate router or additional network appliance shall be required.
IP Stack	Support for IPv4, IPv6, and dual-stack IPv4/IPv6 operation.
Routing Protocols	The proposed SD-WAN solution shall support Static Routing, OSPFv2/v3, BGP (including MP-BGP and Route Reflector functionality where applicable), and Bidirectional Forwarding Detection (BFD) for fast convergence. Support for IS-IS shall be optional for interoperability with service provider networks. Legacy protocols such as RIP/RIPv2 are not required. The SD-WAN edge devices shall support Static Routing, OSPF, BGP, and BFD for branch connectivity and fast failover.
Layer-2 Features	Support for IEEE 802.1Q VLANs; sub-interfaces; logical and virtual interfaces; bridge domains; Ethernet Virtual Connections (EVC); and Port Channel / Link Aggregation using IEEE 802.3ad (LACP).
Security	Support for IPsec; Internet Key Exchange (IKE); where hardware support is available on the proposed platform.
Access & Policy Control	Support for Access Control Lists (ACLs); prefix lists; route maps; and policy-based routing.
QoS & Traffic Engineering	Support for Quality of Service (QoS) including traffic classification, marking, policing, shaping, prioritization, congestion management; policy maps; interface rate limiting (CIR); and storm control.
High Availability	Support for Virtual Router Redundancy Protocol (VRRP).

Network Services	Support for DHCP (client, server, and relay functionality) and DNS client/relay functionality.
Performance	Support for Jumbo Ethernet frames with a minimum MTU of 9000 bytes on LAN and WAN interfaces, as supported by the platform.
Standards Compliance	All features shall be supported using open standards and non-proprietary implementations.

Central Orchestrator / Controller Specifications		
Sr. No.	Technical Requirement	Compliance (Yes/No)
1	The proposed SD-WAN Orchestrator/Controller shall be deployed completely On-Premises . Public Cloud hosted management shall not be acceptable.	
2	The complete management, orchestration, analytics, reporting, policy management and monitoring platform shall be supplied by the same OEM as the SD-WAN solution.	
3	The solution shall support deployment in High Availability (HA) mode without any single point of failure using Active-Active and Active-Standby architecture as supported by OEM with minimum two independent controller nodes with N+N redundancy, deployed across DC and DR, with automatic failover and no single point of failure	
4	Failure of any Controller/Orchestrator node shall not interrupt management, policy synchronization or existing overlay traffic forwarding.	
5	The proposed Central Orchestrator shall support management of minimum 7,800 SD-WAN Edge Devices from Day-1 without hardware or software augmentation.	
6	The proposed architecture shall support future scalability beyond 7,800 devices by addition of controller nodes without replacement of existing hardware.	

7	The solution shall support centralized provisioning, Zero Touch Provisioning (ZTP), template based configuration and policy deployment.	
8	The solution shall support centralized firmware management, software repository, scheduled upgrade, phased upgrade, batch upgrade and rollback.	
9	The solution shall support centralized configuration backup, automated scheduled backup, manual backup and complete restoration.	
10	Configuration version history with rollback capability shall be available for all managed devices.	
11	The solution shall maintain complete audit trail of configuration changes, administrator activities, login history and policy modifications.	
12	The platform shall support Role Based Access Control (RBAC) with Administrator, Read Only, Auditor and Operator roles or equivalent.	
13	The platform shall support integration with LDAP, Microsoft Active Directory, RADIUS and TACACS+ for centralized authentication and authorization.	
14	The solution shall support Multi-Factor Authentication (MFA) for administrative login.	
15	The platform shall support logical segregation (Multi-Tenancy) for different departments/organizations with independent policies and administrative access.	
16	The solution shall support REST API for integration with NMS, SIEM, SOAR, ITSM and third-party applications.	
17	The solution shall support Syslog, SNMPv3, Webhooks and streaming telemetry for monitoring integration.	
18	The dashboard shall provide real-time visibility of device inventory, tunnel status, SLA, bandwidth utilization, application usage, alarms and security events.	
19	The solution shall support application-wise reporting, WAN utilization reports, SLA reports, historical reports and customized reports with export facility.	
20	The solution shall support graphical topology showing SD-WAN fabric, hub, branches, WAN links and tunnel status.	
21	The platform shall continuously monitor Latency, Jitter, Packet Loss and Link Utilization and display SLA compliance for every WAN link.	
22	The platform shall support alarm correlation, event filtering, threshold-based alerts and notification through Email, SMS and Webhook/API.	
23	The solution shall support Certificate Lifecycle Management including certificate generation, renewal, revocation and replacement.	

24	Controller database and configuration shall automatically synchronize between DC and DR locations.	
25	The solution shall support automatic controller failover between DC and DR without manual intervention.	
26	Loss of connectivity to the Controller shall not interrupt branch-to-branch or branch-to-hub traffic. Edge devices shall continue forwarding traffic using last synchronized policy.	
27	The Controller shall support export/import of complete configuration and policy database.	
28	All Controller software, licenses, analytics, reporting, APIs and orchestration features shall remain available during the entire contract period without feature degradation.	
29	The bidder shall provide perpetual/subscription licenses valid for ten (10) years for the complete Orchestrator platform.	
30	The proposed Controller/Orchestrator shall not require any recurring cloud subscription for management functionality.	

SD-WAN HUB CPE Specification		
1	The device / solution should be able to support all the capabilities mentioned under SD-WAN functional requirement	
2	The SD-WAN appliance shall support 20 Gbps SDWAN throughput from day 1 & shall be responsible solely for WAN connectivity, routing, segmentation, application-aware traffic steering, QoS, and IPsec encryption/decryption. The security appliance shall independently support a minimum of 20 Gbps throughput from Day 1 with all required security services enabled.	
3	Device Should support Active / Active & Active-Passive configurations.	
4	All WAN links should be configured in active-active mode across CPE appliances in a site.	
5	The device should have minimum 12X1/10GE SFP+ and 2X40GE QSFP+ ports . The SFP transceivers will be provided by SI as per requirement from same OEM/OEM Authorized Manufacturer of SFP's. The required port density may be achieved through native ports or OEM supported breakout options .All ports should be capable to work as L2 port or L3 ports as per requirement and can be used as both WAN and LAN ports. All ports shall be concurrently usable .	
6	The proposed device may be fixed form factor or modular/chassis-based and shall include redundant hot-swappable power supplies and sufficient redundant cooling/fan modules. The Device must have dual hot swappable AC power supply.	
7	The proposed appliance must support TPM or equivalent in the hardware for secure key encryption.	
8	Should support minimum 10000 overlay IPsec tunnels from day 1.	
9	The device should have minimum 64 GB RAM	
10	The router shall support high availability and the proposed router hardware and software must be stable and production-proven, with no known critical or open Bugs at the time of delivery/Implementation.	
SD-WAN Edge Devices (District HQ) CPE Specification		
11	The device should be able to support all the capabilities mentioned under SD-WAN functional requirement to ensure government branch/department local internet breakout and safe and secure internet service from all locations in case any time request come solution must be ready.	

12	The device should have minimum 10 Gbps of SD-WAN Traffic Throughput from day 1. (After enabling all the security services as mentioned in SD-WAN Key Features). The proposed appliance should support a minimum of 10 Gbps IPsec VPN encryption throughput from Day 1.
13	The device should have minimum 32 GB RAM
14	Device Should support Active / Active & Active-Passive configurations
15	All WAN links should be configured in active-active mode across CPE appliances in a site.
16	The device should have minimum 8X1GE SFP, 8 x1/10GE SFP+ and 4 X 10/25GE SFP28 ports The SFP transceivers will be provided by SI as per requirement from same OEM/OEM Authorized Manufacturer of SFP's. All ports should be capable to work as L2 port or L3 ports as per requirement and can be used as both WAN and LAN ports.
17	The proposed appliance must support TPM or equivalent in the hardware for secure key encryption.
18	The Device must have dual hot swappable AC power supply and sufficient redundant cooling/fan modules
19	Should support minimum 3000 overlay IPsec tunnels from day 1.
20	The proposed hardware and software must be stable and production-proven, with no known critical or open Bugs at the time of delivery/Implementation
SD-WAN Edge Devices (Taluka HQ) CPE Specification	
21	The device should be able to support all the capabilities mentioned under SD-WAN functional requirement to ensure government branch/department local internet breakout and safe and secure internet service from all locations in case any time request come solution must be ready.
22	The device should have minimum 900 Mbps of SD-WAN Traffic Throughput from day 1. (After enabling all the security services as mentioned in SD-WAN Key Features). The proposed appliance should support a minimum of 900 Mbps IPsec VPN encryption throughput from Day 1.
23	The device should have minimum 8 GB RAM
24	Device Should support Active / Active & Active-Passive configurations
25	The device should have a minimum of 8x1G ports, out of which at least 2 ports should be SFP based. Out of the 8 ports minimum 4 WAN and 4 LAN ports should be available. The SFP transceivers of these 2 SFP type ports will be provided by SI as per requirement from the same OEM /OEM Authorized Manufacturer of SFP's.
26	The proposed appliance must support TPM or equivalent in the hardware for secure key encryption.
27	Should support minimum 250 overlay IPsec tunnels from day 1.
28	The proposed hardware and software must be stable and production-proven, with no known critical or open Bugs at the time of delivery/Implementation.
29	The Device must have AC power supply and sufficient redundant cooling/fan modules
SD-WAN Edge Devices (For office location) CPE Specification	
30	The device should be able to support all the capabilities mentioned under SD-WAN functional requirement to ensure government branch/department local internet breakout and safe and secure internet service from all locations in case any time request come solution must be ready.
31	The device should have minimum 500 Mbps of SD-WAN Traffic Throughput from day 1. (After enabling all the security services as mentioned in SD-WAN Key Features). The proposed appliance should support a minimum of 500 Mbps IPsec VPN encryption throughput from Day 1.
32	The device should have minimum 8GB RAM
33	Device Should support Active / Active & Active-Passive configurations
34	The device should have a minimum of 6x1G ports (min. 4 WAN ports), out of which at least 2 ports should be SFP based port. The SFP transceivers of these 2 SFP type ports will be provided by SI as per requirement from the same OEM /OEM Authorized Manufacturer of SFP's.
35	The proposed appliance must support TPM or equivalent in the hardware for secure key encryption.
36	Should support minimum 200 overlay IPsec tunnels from day 1
37	The Device must have AC power supply.

SD-WAN Edge Devices - SIM Based (For office location) CPE Specification	
39	The device should be able to support all the capabilities mentioned under SD-WAN functional requirement to ensure government branch/department local internet breakout and safe and secure internet service from all locations in case any time request come solution must be ready.
40	The device should have minimum 500 mbps of SD-WAN Traffic Throughput from day 1. (After enabling all the security services as mentioned in SD-WAN Key Features). The proposed appliance should support a minimum of 500 Mbps IPsec VPN encryption throughput from Day 1.
41	The device should have minimum 8GB RAM
42	Device Should support Active / Active & Active-Passive configurations
43	The device should have a minimum of 4x1G ports, out of which at least 2 ports should be SFP based port. The SFP transceivers of these 2 SFP type ports will be provided by SI as per requirement from the same OEM /OEM Authorized Manufacturer of SFP's. Additionally device should have inbuilt Dual SIM slots (2 × SIM) supporting cellular connectivity compatible with 3G / 4G / LTE / 5G services, as supported by the device hardware and cellular module. SIM-based SD-WAN CPE shall include cellular modules, dual SIM slots, antennas (indoor/outdoor as required), and all necessary licenses. SIM cards and recurring telecom charges are excluded unless explicitly specified. No additional hardware cost shall be admissible post-award.
44	The proposed appliance must support TPM or equivalent in the hardware for secure key encryption.
45	Should support minimum 200 overlay IPSec tunnels from day 1
46	The Device must have AC power supply.

SECTION 6

PRICE BID

SECTION 6

PRICE BID:

Sr. No.	Product/Item	Quantity Required (A)	Unit Base Price excluding GST (B)	Total Price excluding GST C = AxB
1	Centralized SD-WAN Complete Solution, Orchestrator, Controller with Network Monitoring and centralized management capabilities. (Complete Unit with all hardware, software, license with High Availability with N+N redundancy) at DC and DR location	1		
2	SD-WAN Edge Devices (District HQ)	1		
3	SD-WAN Edge Devices (Taluka HQ & PoP)	1		
4	SD-WAN Edge Devices (For office location)	1		
5	SD-WAN Edge Devices (For office location)-SIM based (LTE/4G/5G)	1		
6	1G SFP – 1000BASE-LX (Single Mode Fiber)	1		
7	1G SFP – 1000BASE-SX (Multi-Mode Fiber)	1		
8	10G SFP+ – 10GBASE-LR (Single Mode Fiber)	1		
9	10G SFP+ – 10GBASE-SR (Multi-Mode Fiber)	1		
10	25G SFP28 – 25GBASE-LR (Single Mode Fiber)	1		
11	25G SFP28 – 25GBASE-SR (Multi-Mode Fiber)	1		
12	40G QSFP+ – 40GBASE-LR4 (Single Mode Fiber)	1		
13	100G QSFP28 – 100GBASE-LR4 (Single Mode Fiber)	1		
14	Remote User Security and Access Management	1		

Following is the notional quantity for reference purpose only:

Sr. No.	Product/Item	Notional Quantity
1	Centralized SD-WAN Complete Solution, Orchestrator, Controller with Network Monitoring and centralized management capabilities. (Complete Unit with all hardware, software, license with High Availability with N+N redundancy) at DC and DR location	1
2	SD-WAN Edge Devices (District HQ)	34
3	SD-WAN Edge Devices (Taluka HQ & PoP)	700
4	SD-WAN Edge Devices (For office location)	5400
5	SD-WAN Edge Devices (For office location)-SIM based (LTE/4G/5G)	100
6	Remote User Security and Access Management	200

- I. All the above-mentioned line items in **Table of the Price Bid** shall fully comply with the functional and technical specifications and the scope of work defined in this RFP, and shall include all applicable licenses, cables, and accessories, as well as installation, commissioning, and configuration charges, along with warranty and onsite support.
- II. Quantities indicated in the Price Bid are for unit rate evaluation purposes only.
- III. Actual quantities shall be finalized at the time of order placement as per project requirements and notional distribution.
- IV. The bidder shall submit a detailed **unpriced Bill of Quantities (BoQ)** for each item/equipment/service proposed under the project, clearly indicating the part codes.
- V. The rates quoted shall remain valid for a period of **Five (5) years** from the date of issuance of the Lol/Work Order. The quoted rates shall be applicable to all line items of the Price Bid. During the rate validity period, DST/GIL may place additional orders, if required at the same rates.
- VI. Non-acceptance of the above conditions or submission of a conditional bid shall result in outright rejection of the bid.
- VII. L1 will be the lowest sum total of rates of all line items excluding GST.
- VIII. Tenderer/GIL may negotiate the prices with L1 Bidder, under each item/head offered by Bidder.
- IX. Any variation / new levy in tax structure levied by State/ Central Govt. shall be taken into account.
- X. Bidder has to mention Applicable tax (GST) and upload separate document for the same. At the time of payment actual Applicable tax (GST) will be paid.
- XI. The rates are inclusive of SITC and FAT at any office across the Gujarat.

SECTION 7

Proof of Concept (POC)

Proof of Concept (POC)

The Tenderer reserves the right to require the **L1 (Lowest Evaluated Responsive Bidder)** to conduct a Proof of Concept (POC) to demonstrate compliance of the proposed SD-WAN solution with the mandatory technical specifications and functional requirements of this RFP.

The POC shall be conducted at a location designated by the Tenderer within **15 calendar days** from the date of intimation and shall be carried out **at no additional cost** to the Tenderer.

The POC shall include, but not be limited to, demonstration of the following:

1. SD-WAN overlay establishment and centralized management
2. Zero Touch Provisioning (ZTP)
3. Application-aware routing and dynamic path selection
4. Automatic WAN failover and failback
5. High Availability and controller redundancy
6. QoS implementation and traffic prioritization
7. IPsec VPN establishment and encryption
8. Security features (Firewall, IPS/IDS, URL Filtering, Malware Protection, etc.)
9. Network analytics, monitoring, reporting, and alerting
10. Role-Based Access Control (RBAC)
11. Compliance with any other mandatory technical requirement specified in this RFP.

The Evaluation Committee shall verify the POC against the mandatory technical requirements of the RFP. The POC shall be **qualifying in nature** and **shall not carry any evaluation marks**.

In the event the L1 Bidder fails to successfully demonstrate compliance with the mandatory technical requirements during the POC, or fails to conduct the POC within the stipulated timeline without valid reasons acceptable to the Tenderer, the Tenderer reserves the right to **reject the bid, forfeit the Bid Security/EMD, if permissible under the tender conditions**, and proceed with the evaluation of the next lowest responsive bidder in accordance with the provisions of the RFP.

The detailed POC test cases, methodology, and acceptance criteria shall be finalized by the Tenderer and communicated to the L1 Bidder prior to commencement of the POC. The POC shall be qualifying in nature and shall not carry any evaluation marks.

SECTION 8

Contract Cancellation / Termination Clause

Contract Cancellation / Termination Clause

1. Termination for Default (Bidder Failure)

The Tenderer may terminate the contract, in whole or in part, by giving **30 days' written notice**, if the Successful Bidder:

- a) Fails to deliver, install, or commission the SD-WAN solution within the stipulated timelines;
- b) Fails to meet SLA requirements or fails to rectify defects within the specified time;
- c) Fails to comply with technical specifications, security requirements, or regulatory guidelines (including CERT-In, DoT, TRAI);
- d) Abandons the project or fails to perform contractual obligations;

2. Termination for Insolvency

The Tenderer may terminate the contract **immediately**, without compensation, if the Bidder becomes:

- a) Insolvent or bankrupt
- b) Subject to liquidation or winding-up proceedings

3. Termination due to Non-Performance in FAT

The Tenderer reserves the right to terminate the contract if:

- a) The Bidder fails to successfully complete **Factory Acceptance Testing (FAT)** after **two attempts**;
- b) Critical requirements (security, failover, compliance, etc.) are not met;

In such case:

- a) Entire order may be cancelled
- b) Performance Security may be **forfeited**

5. Consequences of Termination

Upon termination:

a) The Bidder shall:

- a) Stop all work immediately
- b) Hand over all deliverables, configurations, documentation, and assets

b) The Tenderer reserves the right to:

- a) Get the remaining work completed through alternate agency at **risk and cost of the bidder**

6. Recovery & Risk Purchase

In case of termination due to default:

- a) The Tenderer may procure similar services from alternate sources
- b) Any **additional cost incurred** shall be recovered from the Bidder

7. Blacklisting / Debarment

In case of:

- a) Fraudulent practices
- b) Repeated non-performance
- c) Submission of false information

The bidder may be **blacklisted/debarred** as per Government norms.

8. Partial Termination

The Tenderer may terminate **specific sites / locations / components** without affecting the entire contract.

9. Regulatory Non-Compliance Clause

Non-compliance with directives issued by CERT-In or any statutory authority shall be treated as material breach and may lead to termination.

SECTION 9

Additional document to be submitted & ANNEXURES

SECTION 9

Additional document to be submitted & ANNEXURES

Annexure – B
On Letterhead of Bidder

Please submit the undertaking letter as per Ministry of Finance Memorandum No.: F. No.6/18/2019-PPD dated 23.07.2020 & Office Memorandum No.: F.18/37/2020-PPD dated 08.02.2021 as per Performa given below on OEM letterhead as well as on bidder's letterhead.

Sub: Undertaking as per Office Memorandum No.: F. No.6/18/2019-PPD dated 23.07.2020 & Office Memorandum No.: F.18/37/2020-PPD dated 08.02.2021 & 23.02.2023 published by Ministry of Finance, Dept. of Expenditure, and Public Procurement division

Ref: Bid Number: _____

I have read the clause regarding restriction on procurement from a bidder of a country that shares a land border with India. I certify that we as a bidder and quoted product from the following OEMs are not from such a country or if from such a country, these quoted products OEM has been registered with the competent authority. I hereby certify that these quoted product & its OEM fulfills all requirements in this regard and is eligible to be considered for procurement for Bid number _____.

No.	Item Category	Quoted Make & Model

In case I'm supplying material from a country which shares a land border with India, I will provide evidence for valid registration by the competent authority, otherwise GIL/End user Dept. reserves the right to take legal action on us.

(Signature)
Authorized Signatory of **M/s <<Name of Company>>**

Annexure - C
On Letterhead of OEM

Sub: Undertaking as per Office Memorandum No.: F. No.6/18/2019-PPD dated 23.07.2020 & Office Memorandum No.: F.18/37/2020-PPD dated 08.02.2021 & 23.02.2023 published by Ministry of Finance, Dept. of Expenditure, Public Procurement division

Ref: Bid Number: _____

Dear Sir,

I have read the clause regarding restriction on procurement from a bidder of a country that shares a land border with India. I certify that our quoted product and our company are not from such a country, or if from such a country, our quoted product and our company have been registered with the competent authority. I hereby certify that these quoted products and our company fulfill all requirements in this regard and is eligible to be considered for procurement for Bid number _____.

No.	Item Category	Quoted Make & Model

In case I'm supplying material from a country which shares a land border with India, I will provide evidence for valid registration by the competent authority; otherwise GIL/End user Dept. reserves the right to take legal action on us.

(Signature)

Authorized Signatory of **M/s <<Name of Company>>**

Annexure - D

Performa of Compliance letter/Authenticity of Information Provided

(On Non judicial Stamp paper of Rs. 300 duly attested by the First-class Magistrate/Notary Public)

Date:

To,

GM-Networking

Gujarat Informatics Ltd.

Block No. 2, 2nd Floor, Karmayogi Bhavan,
Sector 10A, Gandhinagar – 382 010

Sub: Compliance with the Tender Terms & Conditions, Specifications and Eligibility Criteria.

Ref: Tender No HWT05082026

Dear Sir,

With reference to above referred tender, I, undersigned <<Name of Signatory>>, in the capacity of <<Designation of Signatory>>, is authorized to give the undertaking on behalf of <<Name of the bidder>>.

We wish to inform you that we have read and understood the technical specification and total requirement of the above-mentioned bid submitted by us on **DD.MM.YYYY**.

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

We also explicitly understand that all quoted items meet technical specification of the bid & that such technical specification overrides the brochures/standard literature if the same contradicts or is absent in brochures.

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

The Information provided in our submitted bid is correct. In case any information provided by us are found to be false or incorrect, you have right to reject our bid at any stage including forfeiture of our EMD/ PBG/cancel the award of contract. In this event, GIL reserves the right to take legal action on us.

Thanking you,

Dated this _____ day of _____ 2025

Signature: _____

(In the Capacity of) : _____

Duly authorized to sign bid for and on behalf of

Note: This form should be signed by authorized signatory of bidder

Annexure - E

Performa of Contract-cum-Equipment Performance Bank Guarantee

(To be stamped in accordance with Stamp Act)

Ref:

Bank Guarantee No.

Date:

To

Name & Address of the Purchaser/Indenter

Dear Sir,

In consideration of <<Name & Address of the Purchaser/Indenter, Government of Gujarat, Gandhinagar>> (hereinafter referred to as the OWNER/PURCHASER which expression shall unless repugnant to the context or meaning thereof include successors, administrators and assigns) having awarded to M/s. _____ having Principal Office at _____ (herein after referred to as the "SELLER" which expression shall unless repugnant to the context or meaning thereof include their respective successors, administrators, executors and assigns) the supply of _____ by issue of Purchase Order No. _____ Dated _____ issued by Gujarat Informatics Ltd. ,Gandhinagar for and on behalf of the OWNER/PURCHASER and the same having been accepted by the SELLER resulting into CONTRACT for supplies of materials/equipments as mentioned in the said purchase order and the SELLER having agreed to provide a Contract Performance and Warranty Guarantee for faithful performance of the

_____ aforementioned contract and warranty quality to the OWNER/PURCHASER, _____ having Head Office at (hereinafter referred to as the 'Bank' which expressly shall, unless repugnant to the context or meaning thereof include successors, administrators, executors and assigns) do hereby guarantee to undertake to pay the sum of Rs. _____ (Rupees _____) to the OWNER/PURCHASER on demand at any time up to _____ without a reference to the SELLER. Any such demand made by the OWNER/PURCHASER on the Bank shall be conclusive and binding notwithstanding any difference between Tribunals, Arbitrator or any other authority.

The Bank undertakes not to revoke this guarantee during its currency without previous consent of the OWNER/PURCHASER and further agrees that the guarantee herein contained shall continue to be enforceable till the OWNER/PURCHASER discharges this guarantee. OWNER/PURCHASER shall have the fullest liberty without affecting in any way the liability of the Bank under this guarantee from time to time to extend the time for performance by the SELLER of the aforementioned CONTRACT. The OWNER/ PURCHASER 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 SELLER, and to exercise the same at any time in any manner, and either to enforce to forebear to enforce any covenants contained or implied, in the aforementioned CONTRACT between the OWNER/PURCHASER and the SELLER or any other course of or remedy or security available to the OWNER/PURCHASER.

The Bank shall not be released of its obligations under these presents by any exercise by the OWNER/PURCHASER of its liability with reference to the matters aforesaid or any of them or by reason or any other acts of omission or commission on the part of the OWNER/PURCHASER or any other indulgence shown by the OWNER/PURCHASER or by any other matter or things.

The Bank also agree that the OWNER/PURCHASER at its option shall be entitled to enforce this Guarantee against the Bank as a Principal Debtor, in the first instance without proceeding against the SELLER and not withstanding any security or other guarantee that the OWNER/PURCHASER may have in relation to the SELLER's liabilities.

Notwithstanding anything contained herein above our liability under this Guarantee is restricted to Rs. _____ (Rupees _____) and it shall remain in force up to and including _____ and shall be extended from time to time for such period as may be desired by the SELLER on whose behalf this guarantee has been given.

Dated at _____ on this _____ day of _____ 2025.

Signed and delivered by

For & on Behalf of

Name of the Bank & Branch &
Its official Address

List of approved Banks

Approved Bank: All Nationalized Bank including the public sector bank or Private Sector Banks or Commercial Banks or Co-Operative & Rural Banks (operating in India having branch at Ahmedabad/ Gandhinagar) as per the G.R. no. EMD/4/2022/0002/DMO dated 20.05.2022 issued by Finance Department or further instruction issued by Finance department time to time

Annexure - F

CONTRACT FORM

THIS AGREEMENT made on the _____ day of _____, 20 ____ Between
_____ (Name of purchaser) of _____ (Country of Purchaser)
hereinafter "the Purchaser" of the one part and _____ (Name of Supplier) of
_____ (City and Country of Supplier) hereinafter called "the Supplier" of the other part:

WHEREAS the Purchaser is desirous that certain Goods and ancillary services viz.,
_____ (Brief
Description of Goods and Services) and has accepted a bid by the Supplier for the supply of those goods and services
in the sum of _____ (Contract Price in Words and Figures)
hereinafter called "the Contract Price in Words and Figures" hereinafter called "the Contract Price."

NOW THIS AGREEMENT WITNESSETH AS FOLLOWS:

- 1 In this Agreement words and expressions shall have the same meanings as are respectively assigned to them in the Conditions of Contract referred to.
- 2 The following documents shall be deemed to form and be read and construed as part of this Agreement, viz. :
 - 2.1 the Bid Form and the Price Schedule submitted by the Bidder;
 - 2.2 terms and conditions of the bid
 - 2.3 the Purchaser's Notification of Award
- 3 In consideration of the payments to be made by the Purchaser to the Supplier as hereinafter mentioned, the Supplier hereby covenants with the Purchaser to provide the goods and services and to remedy defects therein in conformity in all respects with the provisions of the Contract.
- 4 The Purchaser hereby covenants to pay the Supplier in consideration of the provision of the goods and services and the remedying of defects therein, the Contract Price or such other sum as may become payable under the provisions of the Contract at the times and in the manner prescribed by the Contract.
- 5 Particulars of the goods and services which shall be supplied / provided by the Supplier are as enlisted in the enclosed annexure :

TOTAL VALUE:

DELIVERY SCHEDULE:

IN WITNESS whereof the parties hereto have caused this Agreement to be executed in accordance with their respective laws the day and year first above written.

Signed, Sealed and Delivered by the

Said _____ (For the Purchaser)

In the presence of _____

Signed, Sealed and Delivered by the

Said _____ (For the Supplier)

In the presence of _____

ANNEXURE - I

Bid Processing Fees and Earnest Money Deposit Details

Sr.	Item	Amount (In	Name of the Bank and	Demand Draft
1	Earnest Money Deposit (E.M.D.)			

ANNEXURE - II

Form No. E1 Experience in supply, installation commissioning and maintenance of the similar Systems

Name of the Bidder:							
Sr. No.	Name of Organization	Address of the installation	Start date of the project	Completion Date of the Project	Scope of the work. Also specify the system installed	Specify No. of Active and Passive Components	Value of the project in Rupees
1							
2							
3							
4							
5							

Note: Please attach purchase order/ contract agreement and completion certificate for each of project details mentioned

Form no. E2 Authorization Letters

Sr.No.	Item	Make and Model	Name of OEM	Authorization letter attached? (Yes/No)
1				
2				
3				

Format: For MAF / OEM Authorization.

No. _____ dated _____

To

Ref: Tender No. _____

Subject: _____

Dear Sir,

We, _____ who are established and reputed Manufacturers of _____ having factories at _____

_____ (address of factory) do hereby authorize
M/s. _____
_____ (Name & Address of agent) to submit a bid, and sign the contract with you against above mentioned
tender No: _____.

We authorized the _____ (name of the bidder) for the following modules/products:

Sr. No.	Product Name	Make & Model
1		
2		
3		

We hereby confirm that the offered Product in the referenced RFP will be provided unconditionally with a back to back warranty, maintenance, support services and parts availability etc. for proposed product etc. available for the period of five years from FAT through M/s _____ (SI/Bidder).

Yours faithfully,
(Name)
(Name of manufacturers)

Form no. E3 Office in GUJARAT

Sr. No.	Address	Contact Person	Contact nos.	Type of supporting
1				
2				
Note: You may mention more than one office (if applicable)				

Form no. E4 Service Centers Detail

Sr. No.	Address	Contact Person	Contact nos.	Type of supporting
1				
2				
3				
Note: You have to mention minimum 3 authorized service centers as per eligibility criterion. You may add more service centers (if applicable)				

Form No. E5 Bidder Turnover

Financial Year	Annual Turn Over	Related Annual turnover (as per eligibility Criteria)	Audited Accounts submitted? (Yes/No)
2022-2023			
2023-2024			
2024-2025			

Note: Please fill this form and attach the audited Annual Accounts for the last three financial years. (bidder have to submit CA certificate for the same)

Form no. E6 ISO 9001:2008 and 14001:2004 certification for Manufacturing

Sr. No.	Item	Make and Model	Name of OEM	ISO certification valid up to	ISO certification attached? (Yes/No)
1					
2					
3					
4					
5					
6					
7					

Form no. E7 Check list for FAT (Final Acceptance Test)

Sr. No.	Item	Remarks
1	Device Should be configured as per GOG instruction.	
2	Bill of Materials details	
3	Customer Site completion/testing report.	

End of the Document
