भारत संचार निगम लिमिटेड
(भारत सरकार का उपक्रम)
BHARAT SANCHAR NIGAM LIMITED
(A Govt. of India Enterprise)

कार्यालय मुख्य महाप्रबन्धक,उत्तर प्रदेश (पूर्वी) परिमंडल,हजरतगंज लखनऊ।

पत्रांक संख्या: UPE/OP/PM WANI/Correspondence/2022-23/
दिनांक: 25-11-2023

30-03-2024

नोटिस

वाई-फाई हॉट-स्पॉट (पब्लिक डाटा ऑफिस,PDO) के अवस्थापन हेतु आवश्यक सूचना

सर्वसाधारण की जानकारी हेतु प्रेषित किया जा रहा है कि बीएसएनएल ने **वाई-फाई हॉट-स्पॉट (पब्लिक डाटा ऑफिस,PDO) के अवस्थापन हेतु** एक ओपेन-पॉलिसी जारी की है जिसका उद्देश्य भीड़-भाड़ वाली जगहों जैसे बाजार, मॉल, अस्पताल, सरकारी एवं गैर सरकारी भवन, व्यसायिक स्थल, बहुमंजली इमारत, कैफ़, किराना स्टोर इत्यादि पर तीव्र इंटरनेट प्रदान करना है।

इस योजना के अंतर्गत मॉडल –II से जुडने के लिए सहायक महाप्रबंधक (प्रचालन) बीएसएनएल पूर्वी परिमण्डल कार्यालय हज़रतगंज लखनऊ में संलग्न EOI की प्रविष्ठियाँ पूर्ण रूप से भरकर उपुक्त संलग्नों के साथ संपर्क करें।

इस योजना मे ज्यादा से ज्यादा संख्या मे जुड़कर भारत सरकार की डिजिटल इंडिया मिशन मे भागीदार बने।

संलग्न : EOI पत्रावली

30-03-2024

उप महाप्रबंधक (प्रचालन-सीएफ़ए)

BHARAT SANCHAR NIGAM LIMITED
O/o Chief General Manager
UP East Circle

Expression of Interest
for
Public Wi-Fi Partners for provisioning of PM WANI Compliant Wi-Fi Hotspots under Model-II of BSNL Wi-Fi Policy in UP East Circle (Business Area/Operation Area).

EOI No: ..... Dated: ..../..../20...

Signature of Bidder.....

Name of Bidder.....

Last date of submission/Date of opening of Bid.....

This document contains ...40.... pages including the cover page. Please check that all the pages are intact in the document.

CHECK LIST FOR BIDDERS / APPLICANTS.

1. The Bidder should ensure that all documents and papers submitted in this EOI are fully authenticated by the authorized signatory under his signature with official seal wherever applicable.
2. The following documents form part of the EOI and should be submitted with EOI:

Sl. No.	Documents to be submitted	Documents submitted	
		Y / N	Page No. at which Document Attached
1	All pages of this EOI document, duly signed by the authorized signatory in a token of acceptance of all terms and conditions by the bidder. Any other document submitted by the bidder should also be signed by the authorized signatory.		
2.	Duly filled application form for companies/firms/PWPs/SI/TIP/Bharat Udyami & FTTH partners along with annexures.		
3.	General Power of attorney in favor of the signatory signing the EOI documents. It is not required in case of proprietary/partnership firm/BSNL PWP/SI/TIP/FTTH Partner himself signs the documents.		
4.	Attested copy of Article or Memorandum of Association or partnership deed or proprietorship registration or partnership letter awarded by BSNL for PWP ship/FTTH partnership/TIP/SI as the case may be.		
5.	Attested copy of LST/GST Registration number, if applicable.		
6.	Attested copy of PAN/GIR Number.		
7.	Attested copy from CA of turn over details for the year 2020-21,2021-22 & 2022-23 (P&L Account) Turnover certificate item wise.(as per eligibility if required)		
8.	Certificates for experience with telecom service provider(s)/ISP for minimum one year as on the date of opening of EOI.		
9.	Latest Income Tax clearance certificate/Acknowledgement receipt		
10.	Any other supporting documents as asked for or called for.		

3. Every additional document submitted and every page of the EOI document shall be duly signed by the authorized signatory as a token of compliance and acceptance to all terms and conditions.

TABLE OF CONTENTS.

Bharat Sanchar Nigam Limited
O/o Chief General Manager
UP East Circle

NOTICE INVITING EOI (Expression of Interest) for Public Wi-Fi Partners (PWPs) for provision of Wi-Fi services in UP East Circle under BSNL Wi-Fi Open Policy (Model-II) .

EOI No. .....

Sealed EOI are invited by Chief General Manager UP East Circle on behalf of BSNL for selection of PWP to design, build, operate & maintain the Wi-Fi services to provide High Speed Internet Services with wireless network at its own cost at various locations in UP East Circle, from eligible and willing parties (Public Wi-Fi Partners)

TERMS & CONDITIONS
PART-I

COMMERCIAL CONDITIONS

1. **Scope of the Work**: Broad level scope of work of PWP shall be as below:

1.1 PWP shall design, build, operate and maintain the system to provide High Speed Internet Services with wireless network at its own cost. The offered Wi-Fi hotspot equipment shall conform to international standards.

1.2 PWP shall supply, install & commission Wi-Fi Hotspots equipment **(AP-Access Point, PoE Switch/CCU/Router, UPS & Battery, cables along with all the required accessories etc).** After installation and commissioning of the equipment PWP shall operate and maintain the services 24*7 round the clock basis.

1.3 PWP shall supply, install and maintain the equipment such as WLC, EMS/CMS /Captive portal, OCS which should compatible with BSNL Wi-Fi core(WAG). NOC support with EMS for managing Access Points (APs) at Hotspot locations shall have to be provided as well.

1.4 WLC shall be Wi-Fi Certified for TM (Release 2 and above), It should have proven and security hardened operating system and shall provide network services like QOS, 802.1Q, WPA, WPA2 etc. Security guidelines of DOT/ government of India/ Regulatory authority issued from time to time shall be adhered to.

1.5 PWP shall provide Voucher management system for selling pre-paid vouchers on the hotspots and shall also provide comprehensive and flexible Billing capabilities and authentication techniques for its customers with back end systems for authentication, authorization, accounting, security management, network management, billing and customer provisioning & management.

1.6 Compliance to all mandatory government of India regulations and security guidelines and providing information to Law Enforcement Agency (LEA), Data storage and compliance to LIM & security related requirements shall be the responsibility of PWP.

1.7 PWP shall carry out integration of their Captive Portal with BSNL Payment Gateway for different types of digital payment service such as UPI, e-Wallets, Credit and Debit Cards, Online Banking etc.

1.8 PWP shall set up call Centre for dealing with customer requests/complaints related to hot spot services and also extend mechanism for Web support and provide SLA monitoring tools and related infra. Space and Power Supply for call center shall be made available by BSNL free of cost.

1.9 PWP shall Set-up, Deploy, Own and Operate all the hardware & connectivity at hotspot locations with CAPEX and OPEX on part of PWP. They should manage Operations and Maintenance (O&M) at the hotspot locations.

1.10 The equipment shall be commissioned after successful acceptance testing by BSNL Wi-Fi NOC.

1.11 PWPs shall ensure that technology awareness about the Core and Central equipments deployed by PWP are made available to BSNL Wi-Fi NOC team. User id, passwords and subsequent changes for system access and configuration shall be made available to NOC-in charge.

2. BSNL's Responsibilities:

(i) BSNL Core systems (Captive portal, AAA, charging platform, etc).
(ii) Lawful Interception & Monitoring and regulatory compliance.
(iii) Support at BSNL Core and RPOP for configuration, O&M of the PWP deployed equipment.
(iv) Agreement with OEM of WLC and access systems at BBNW NOC for Wi-Fi Hotspots of PWP.
(v) Revenue share arrangement settlement platform and commission for transactions.
(vi) Branding of the services.
(vii) Sales and marketing efforts for roping in new enterprise customers on bulk plans.

3. Migration of Existing Hotspot Location Service Providers (HSSPs) into the agreement:

3.1 Existing Hotspot Service providers (HSSP) of BSNL who have revenue share contract with BSNL on non-exclusive basis can also be migrated into Wi-Fi Open Policy. The prevailing Wi-Fi Core and Access Infrastructure of HSSPs shall be migrated into new policy after the signing of the agreement. In such cases, PWPs shall ensure hardware/software/technology in use is not obsolete/end of life and necessary upgrades/patch are promptly applied. Technical compliance for the same shall be ascertained by BBNW Circle.

4.

BSNL reserves the right to suspend the services in case content is outdated/ obscene/ or offending to the feelings of any religion or community against the Law or un-satisfactorily responsive.

5. Duration of Agreement and extension thereon:

5.1 Duration of contract shall be 3 years from the effective date of signing of the agreement which includes **3 months of deployment timeline.** After 3 years, the contract can be extended in the block of 2 years on satisfactory service to customer.

5.2 Renewal or extension of the agreement after 3 years period will be based on the performance of the PWP.

5.3 There shall be lock in period of minimum 3 years for the PWP in order to ensure maintenance unless BSNL terminates the contract, the bidder is bound to provide services for 3 years. The exit during lock in period shall carry penalty in terms of surrender of all the equipment to the BSNL at no cost.

5.4 After completion of 3 years if PWP wants to exit, he needs to surrender all the equipments

6. Provision of Service:

6.1 PWP shall plan, install & commission & carry out O&M of Wi-Fi Hotspots at various locations at its own cost for provisioning of Wi-Fi services under this Agreement.

6.2 PWP shall also be responsible for obtaining the copyrights and complying with the Intellectual Property Rights of the content, wherever applicable. PWP shall indemnify BSNL in respect of any consequences of whatsoever nature arising on account of copyright violation of content or content being in violation of laws of land.

6.3 It is specifically agreed by PWP that it shall, at no point of time, use the services and/ or the connectivity under this agreement for push messaging.

6.4 PWP shall provide help-line/ help-desk/ Customer care centers/ customer care line for fault rectification, handling service disruption/ de-gradation, etc. round the clock, seven days a week and 365 days a year.

6.5 The helpdesk shall be located in BSNL premises where Central Equipment(s) of PWP are operational. BSNL shall provide space for the same.

7. Last Mile Connectivity:

Plans	BW to Customer Premises	Connectivity Type	Charges for BW
Retail	BSNL shall extend till PDO premises.	FTTH/AirFiber	Monthly rental plans to be paid by PDOs to BSNL.
Bulk/ Enterprise	BSNL shall extend BW, any extra expenditure incurred by BSNL on last mile, shall be billed to the customer and there shall be no revenue share on this with PWP.	Available FTTH Plans	To be billed in FTTH Plans.

8. Delivery of Service

PWP shall ensure provisioning of commercial services within 3 months from date of signing of agreement. BSNL may terminate agreement in the event failure to commission the equipment and/or execution of work by PWP. However, delay on account of BSNL shall be taken due care of while calculating 3 months time.

9. Marketing of Services

9.1 For Enterprise Wi-Fi Solution, Enterprise Sales Team shall be appointed by Partner to work along with BSNL sales team, for improving the growth of Enterprise Wi-Fi business in BSNL.

9.2 For Retail Wi-Fi Business, PWPs shall work on non-exclusive basis and shall engage PDOs by explaining business model. They should also technically train the PDO on self-service portal to understand the voucher sales and revenue earned.

9.3 **Roles and responsibilities of PDOs**:

9.3.1 Public Data Office PDO, is the acronym used for Retail Hotspot locations such as retail shops may be tea/coffee/groceries where good number of foot-falls are involved.

9.3.2 PDOs partners shall work in conjunction with PWP. BSNL will have revenue share arrangements with PWPs only. PWP shall in turn share revenue with PDO partners through their direct arrangements.

9.3.3 PDO shall be responsible for housing the Wi-Fi Equipment, providing housing & power, First level maintenance and sale of Recharge coupon /Voucher through mobile app.

9.3.4 PDOs shall be mandatorily asked by PWPs to install Back-Lit sign boards at PDO premises with BSNL logo so that presence is felt in the vicinity. Appropriate design for the same shall be issued by BSNL.

9.4 In case of retail plans, PWPs shall provide vouchers to PDOs for selling through the mobile app. PWPs shall offer voucher denominations specific to geography and anticipated demand so as to tap market potential and generate leads. Vouchers to PDOs, shall be with the approval by BSNL.

9.5 Mobile app for sale of recharge vouchers shall be given by BSNL and PWPs shall enable PDO for easy sale of recharge vouchers and activation of subscribers for retail plan.

10. Roles and responsibilities of PWPs:

1. BSNL will register FTTH Partners/Cluster Partner/SIs having good record of services in working in BSNL's last mile network, as PWP under this Model.
2. The PWP will supply, install, commission, operate and maintain Wi-Fi access points with all associated accessories.
3. This partnership and shall have back to back arrangement with OEM of AP/WLC.
4. The Access points shall be integrated with respective OEM WLC for which OEM agreement is in place at BBNW NOC Bangalore.

11. Modifications in the Terms and Conditions of Agreement

The terms and conditions of the Agreement are subject to modification by mutual agreement based upon the request of either party. Notwithstanding anything contained herein, the revenue share to PWP and other related conditions may be changed upon mutual consent of both the parties.

12. Subcontracts

The PWP shall not sub-contract the work assigned to him to any other party, without prior permission of BSNL. Such sub-contracts, if any, shall not relieve PWP from any liability or obligation under the conditions of the agreement. PWP shall be responsible for completion of the work and liable for performance and adherence to the terms and conditions of the Agreement.

13. Suspension, Revocation or Termination of agreement

13.1 The agreement shall be terminated by giving a one month's notice to the PWP in case of:

(i) Failure to commission the equipment and/ or execution of the work at all by the PWP within 3 months from signing of agreement, excluding the cases where reasons for delay in the commission of equipment and/ or execution of works are attributed to BSNL.

(ii) Failure to perform any other obligation(s) under the Contract; and equipment does not perform satisfactory in the field in accordance with the specifications.

(iii) Failure to meet the SLAs parameters (as per SLA agreement between BSNL and customer for enterprise business continuously for 3 month.

13.2 BSNL may at any time terminate the Contract by giving written notice to PWP without compensation to PWP, If:

(i) PWP becomes bankrupt or otherwise insolvent as declared by the competent court provided that such termination shall not prejudice or affect any right of action or remedy which has accrued or shall accrue thereafter to BSNL.

(ii) There is a failure to meet the compliances as required by DOT/ Regulatory/Lawful agencies.

13.2.1 In such termination BSNL shall take over the business, with all the Core equipment and access equipment (owned by PWP) at no cost to PWP. BSNL may either choose to empanel third party for operation and maintenance of such equipment for serving existing customer or maintain on its own.

13.3 The agreement may also be terminated after lock in period of 3 years through mutual written consent of both parties by giving 3 months' notice. On termination of agreement the customers shall continue to use the Telecom services of BSNL, through commissioned equipment under the contract. However the entire business, i.e. customer services along with all equipments can be transferred from existing PWP to other eligible PWP of their mutual agreement, with fresh agreement with BSNL by new PWP by producing valid NOC from existing PWP existing PWP.

14. Actions pursuant to Termination of Agreement

14.1 There shall be lock in period of minimum 3 years for the PWP in order to ensure maintenance unless BSNL terminates the contract, the bidder is bound to provide services for 3 years. The exit during lock in period shall carry penalty in terms of surrender of all the equipment to the BSNL at no cost.

14.2 In case of termination pursuant to clause 13, BSNL shall take over the business, with all the WLC/EMS/ CMS equipment and access equipment (owned by PWP) at no cost to PWP. BSNL may either choose to empanel third party for operation and maintenance of such equipment for serving existing customer or maintain on its own.

14.3 On termination or surrender or expiry of the Agreement, **PWP** shall ensure clearance of dues, if any, which it is liable to pay to BSNL. In case of failure to pay the amounts due to BSNL, the outstanding amounts shall be realized through the pending bills due to **the PWP** without prejudice to any other action(s) for recovery of the amounts due to BSNL or from the performance Bank Guarantee submitted by the PWP.

15. Dispute Settlement

The dispute settlement/arbitration shall be as per Annexure II. The venue of the arbitration proceeding shall be Lucknow,U.P.

16. Force- Majeure

If at any time, during the continuance of this agreement, the performance in whole or in part, by either party, of any obligation under this is prevented or delayed, by reason of war, or hostility, acts of the public enemy, civic commotion, sabotage, Act of State or direction from Statutory Authority, explosion, epidemic, quarantine restriction, strikes and lockouts, fire, floods, natural calamities or any act of God (hereinafter referred to as **event**), provided notice of happenings of any such event is given by the affected party to the other, within 21 Calendar days from the date of occurrence thereof, neither party shall, by reason of such event, be entitled to terminate the agreement, nor shall either party have any such claims for damages against the other, in respect of such non-performance or delay in performance. Provided Service under the agreement shall be resumed as soon as practicable, after such event comes to an end or ceases to exist. The decision of BSNL as to whether the service may be so resumed (and the time frame within which the service may be resumed) or not, shall be final and conclusive. However, the Force-majeure events noted above will not in any way cause extension in the period of the agreement.

17. Right to inspect

17.1 BSNL or its authorized representative shall have right to inspect the sites used for extending the Service by **PWP** and in particular but not limited to, have the right to have access to leased lines, junctions, terminating interfaces, hardware/ software, memories of semiconductor, magnetic and optical varieties, wired or wireless options, distribution frames, and conduct the performance test including to enter into dialogue with the system through Input/ output devices or terminals. **PWP** will provide the necessary facilities for continuous monitoring of the system, as required by BSNL or its authorized representative(s). The inspection will ordinarily be carried out after reasonable notice except in circumstances where giving such a notice will defeat the very purpose of the inspection.

18. Confidentiality

18.1 Subject to conditions contained in this Agreement, PWP shall take all necessary steps to safeguard the privacy and confidentiality of any information about BSNL and its subscribers from whom it has acquired such information by virtue of the Service provided and shall use its best endeavors to secure that:

18.1.1 No person acting on behalf of PWP or PWP himself divulges or uses any such information except as may be necessary in the course of providing Services to BSNL; and

18.1.2 No person seeks such information other than is necessary for the purpose of providing Service to BSNL.

18.1.3 Provided, the above Para shall not apply where BSNL has consented in writing to such information being divulged or used, and such information is divulged or used in accordance with the terms of that consent; or the information is already open to the public.

18.1.4 This clause shall survive the termination or expiry of this Agreement.

19. Set Off

Any sum of money due and payable to PWP under this Agreement or otherwise shall be appropriated by BSNL and the same may be set off against any claim of BSNL for payment of a sum of money arising out of this Agreement or under any other Agreement made by PWP with BSNL.

20. Indemnification:

20.1 PWP shall agree to protect, defend, indemnify and hold harmless BSNL and its employees, officers, directors, agents or representatives from and against any and all liabilities, damages, fines, penalties and costs (including legal costs and disbursements) arising from or relating to:

20.1.1 Any breach of any statute, regulation, direction, orders or standards from any governmental body, agency, telecommunications operator or regulator applicable to such party;
20.1.2 Any breach of the terms and conditions in this agreement by PWP;
20.1.3 Any claim of any infringement of any intellectual property right or any other right of any third party or person or of law by PWP;
20.1.4 Any claim made by any third party or person arising out of the use of the services and arising in connection with interruptions or degradations of service caused solely by PWP.

21. Relationship

Each party understands that it is an independently owned business entity and this Agreement does not make it, its employees, associates or agents as employees, agents or legal representatives of the other party for any purpose whatsoever. Neither party has express or implied right or authority to assume or to undertake any obligation in respect of or on behalf of or in the name of the Other Party or to bind the Other Party in any manner. In case, any party, its employees, associates or agents hold out as employees, agents or legal representatives of the other party, the former party shall forthwith upon demand make good any/ all loss, cost, damage including consequential loss, suffered by the other party on this account.

22. Non-Exclusivity:

This Agreement is non-exclusive and nothing in this Agreement will be construed to prevent either party from entering into a similar Agreement with any other party or to restrict such party from directly engaging in related activities.

23. Liability

Except as provided in this Agreement, hereinabove, neither party shall be liable to other party or any other party by virtue of termination of this Agreement for any reason whatsoever for any claim for loss or profit or on account for any expenditure, investment, leases, capital improvements or any other commitments made by the other party in connection with their business made in reliance upon or by virtue of this Agreement.

24. Intellectual Property Rights/ Copyrights.

24.1 The Intellectual Property Rights of BSNL and the **PWP** shall remain their own and this Agreement shall not affect their ownership in any way unless mutually agreed upon.

24.2 **PWP** shall be responsible for obtaining the legitimate copyrights/ Intellectual Property Rights of the content provided as part of the services agreed upon under this Agreement.

24.3 **PWP** indemnifies BSNL against any liability, damage, fine, penalty, costs or any other consequential loss on account of violation of the copyright/ Intellectual Property rights of any third party by **PWP** in respect of the content/ application/ technology used by **for** providing the services.

24.4 **PWP** shall ensure that no profiling information regarding the Wireless subscribers of BSNL using these services is collected, analyzed, sold, transferred or otherwise disclosed to any third party or utilized for the purpose of promoting the other than agreed products/ services.

24.5 **PWP** shall not use BSNL's trademarks, trade names, service marks, copyrights, patents, trade secrets, trade dress or BSNL Logos, etc. without BSNL's prior written consent.

24.6 Notwithstanding anything contained herein, **PWP** indemnifies and hold BSNL harmless against any loss, liability, costs (including legal costs & expenses), fine, penalty, demands or damages arising by reasons of any claim of infringement, passing off or dilution of IPR/ copyright/ patent/ trademark/ etc. arising from provision of services under this agreement and use of same or any part thereof by BSNL or by subscribers of BSNL or in Telecom Network of BSNL, as the case may be.

25. Compliance to Applicable Law

25.1 Security Requirements: PWP shall sign security agreement as per Annexure-IV of the agreement.

25.2 PWP shall enable the BSNL to comply with Applicable Laws including but not limited to notifications, circulars etc issued by DoT from time to time.

25.3 Compliance with Licenses: PWP shall assist and provide support as and when required to BSNL including the providing of information and documents to comply with the provisions of the Licenses, any

amendments made thereto as well as any notifications, circulars, directions/regulations issued by DoT/TRAI or any other Governmental Authority from time to time specially in relation to security clearance and lawful interception.

25.4 **Non-Compliance:** PWP including their personnel, employees, associates and sub-suppliers shall be solely responsible for complying with the statutes, laws, regulations, subordinate legislation, administrative orders and instructions issued by relevant Government Authorities, regarding, but not limited to, environment, industrial relations, security and taxation, during the performance of their respective obligations under this Contract. Without limiting the generality of the foregoing, the Supplier shall be responsible for compliance with the Applicable Laws and similar regulations applicable to its activities hereunder, at its own cost and expenses.

26. **Revision in policies:**

BSNL reserves the right to make any changes in various policies including but not limited to marketing, penalties for forced activation of subscriber's services, allocation of network and other infrastructure resources. BSNL reserves all rights to incorporate changes in the policies from time to time, under intimation to PWPs. Decision of BSNL will be final and to that extent, the agreement along with Annexures shall be deemed to have been modified or amended.

PART-II

FINANCIAL CONDITIONS

1. **Revenue from the Services:**

1.1 Definition of revenue:

1.1.1 Enterprise Wi-Fi/Bulk User services:

i. For post-paid Enterprise Wi-Fi Bulk Users, revenue will be amount billed to enterprise customers exclusive of GST. SLAs and specific terms and conditions, if any, agreed with Enterprise customers shall be applied back to back with the PWP.

ii. The revenue share in enterprise Wi-Fi service shall be on net realized revenue i.e. after deducting taxes as applicable.

iii. The revenue share will be on net revenue (after deduction of GST and other tax). Presently these Wi-Fi services are provided under ISP license.

1.1.2 Retail Wi-Fi Services:

i. For retail models, revenue shall be sale value of the Wi-Fi recharge wallet stock sold to the PWP, exclusive of GST.

ii. Share of Wi-Fi recharge wallet stock to PWP shall be provided in terms of discounts on the wallet.

iii. Commercial arrangement between PWP and PDOs under retail plans shall be decided by PWP based on level of enablement done by PWP to the PDO partner and BSNL will not have any role to play.

2. **Revenue share/Discounts for bulk/enterprises services:**

2.1 Following Revenue share for bulk/enterprise plans shall be applicable:

Revenue Share to the PWP in Bulk plans (Model-II)	**50%**

* Revenue shares or discounts for models as above for Retail Wi-Fi Business and Enterprise Wi-Fi Business are kept same as infrastructure and related services involved are the same.

2.2 **After 2 years (from the start of 1st Wi-Fi hotspot commercialization for that partner), for subsequent years, the revenue share/discounts ofered to PWP in model-II will be reduced to 45%.**

2.3 Commercial arrangement between PWP and PDOs under retail plans shall be decided by PWP based on level of enablement done by PWP to the PDO partner and BSNL will not have any role to play.

2.4 The revenue share % should be limited to 2 decimal points only. Any figure after 2 decimal points shall be ignored for all purpose.

2.5 In case of variation between revenue share % mentioned in figures & words, the Revenue share % mentioned in words shall prevail.

2.6 The revenue share will be on net revenue (after deduction of GST and other taxes). No AGR related deductions to be made in revenue share

3. **Discounting Process Flow for Retail Business:**

i. The commercial arrangement with PWP in retail plans shall be on P2P basis (Principal to Principal), as done in C-top up wallet system for Mobile.

ii. PWPs will purchase the wallet balance in advance from BSNL.

iii. The customer visiting the HOTSPOT of PDO will purchase a Wi-Fi Data pack. On Purchase of data pack using online channel, money will be received by the PWP and the PWP wallet will be deducted while in case of direct sale at PDO, money received from the customer is paid to PDO and the wallet will be deducted with an equal amount. The mechanism of invoice sale from PWP to PDO or customer will be handled by PWP only.

iv. Discounts to PWP as per various models will be provided upfront at the time of wallet purchase.

4. **Revenue share Process Flow & payment procedure for Bulk/Enterprise Business:**

i. Once an enterprise Customer is acquired by PWP, the details of tarif plans and related information, shall be entered in BSNL's IT system.

ii. The plan confguration and Billing for Bulk customers is already available in CDR System. Accordingly, the revenue share and Tagging of the Public Wi-Fi Partner shall be done in the CDR systems.

iii. The revenue share reports shall be published in CDR / FMS system. FMS system shall provide Revenue Report by taking annual payments, cancellation and refunds into account. The Revenue Report is generated after realization of revenue for any given enterprise customer.

iv. After generation of revenue reports on FMS , Payment of Bills to PWPs shall be made centrally at Circle level, based on the online Report of Revenue Share. One central location in the circle shall be responsible for the payment of all PWPs in the circle and payment shall be made within one month from realization of revenue from enterprise customer.

v. In the enterprise WiFi, customers shall be billed in advance for the annual charges. The PWP partner can be paid revenue share on quarterly basis for 25% of the annual charges for first three quarters. In fourth quarter the charges shall be paid after settlement of SLA/related penalties agreed with customer.

vi. Rebates and compensation given by courts/TRAI/ any regulatory body to the customers, due to service defciency, if any, shall be deducted from the due payment to the channel partner.

vii. Any discrepancy found in the payment settlement shall be mutually discussed and resolved. Balance of payments arising due to any reason shall be adjusted in future. In case of bill cancellation (due to wrong billing etc.) later, any excess payment made paid to Public Wi-Fi Partner (PWP) shall be adjusted accordingly on quarterly basis.

viii. For the Wi-Fi bulk user plans, the SLAs agreed with customers shall be applied back to back on the PWP. However, the Public Wi-Fi Partner shall not be levied penalty for faults on part of BSNL.

ix. PWPs shall submit the quarterly revenue share invoices to the Nodal of the Circle within 5 days after generating the invoices.

x. BSNL shall not pay any charges in advance. Bills for revenue share of PWPs shall be paid by BSNL at the end of each quarter, after successful execution of the works under this Agreement & fulfilling the SLA benchmark.

xi. BSNL reserves the right to adjust any over-payment of in any quarter.

xii. All payments shall be made by the BSNL circle centrally based on the uptime report from Wi-Fi Core, NOC & portals from Node-in-charges, meeting the SLA parameters after deducting penalty if any.

xiii. The Nodal Circle shall monitor the distribution of funds strictly so as to avoid any transfer of advance before provisioning of services at Bulk User premises.

5. **Enterprise Plans and modifications:**

i. Plans as per provisions of Wi-Fi Open Policy available at www.bsnl.co.in shall be applicable for offering to Bulk User Customers.

ii. New plans shall be introduced as per prevailing market conditions.

iii. Any discounting power for these plans shall be decided by BSNL Corporate Office with the approval of Director (CFA).

6. **The Eligibility conditions of the PWP shall be as under:**

i. Any registered/partnership/proprietorship firm/Society including existing Telecom Infra provider, having minimum turnover of Rs 2 lakhs per year during the last three consecutive years shall be eligible.

ii. The registered/partnership/proprietorship firm/Society shall have worked with Telecom Service Provider(s)/ISP(s) for minimum 1 year.

iii. Existing FTTH Franchisee/Franchisee/Cluster Partners with good record of providing FTTH connections/BSNL services shall be eligible to become Public Wi-Fi Partners (PWP).

Or

Existing TIP/Bharat Udyami in BSNL with annual average FTTH connection 500 in a year along with revenue* (before sharing) of 20 lakh in one circle.

(average FTTH connection in April and March of same financial year.)

Or

Existing System Integrator (SI)/BSNL empaneled IT related service provider having 5 project running/completed.

Or

Any existing Hotspot service provider emplaned with BSNL under Model-III/Model-II.

7. **Empanelment Fee: PWP shall be required to submit an non-refundable empanelment fee of Rs. 10000/- plus applicable taxes along with the agreement in the form of DD in favour of Accounts Officer (Cash, BSNL Circle Office, Hajratganj, Lucknow).**

8. **Access points of PWP shall be integrated with respective OEM of WLC. The copy of the agreement between BBNW NOC Bangalore & OEM/Authorized representative of OEM of Public Wi-Fi Partner (PWP) must be submitted to this office before signing this agreement.**

PART-III

TECHNICAL CONDITIONS

0

1. Wi-Fi Core System/WLC shall have following broad level functionalities:

1.1 Wi-Fi Offload and Service Management Platform (SMP): This platform for management of Wi-Fi subscribers and their service packages along with their login credentials and policies. This platform is integrated with BSNL packet core network components of HLR, IN/OCS, Mediation, PCRF, Payment Gateway, SMSC and Email System and with BSNL wire line broadband network components of broadband network AAA, Policy Manager, Mediation. This system also supports rating and charging of walking/guest users which is to be performed differently from offload users.

1.2 **Captive Portal:** Users connect to BSNL Wi-Fi SSID and upon receiving IP Address are re-directed to a PORTAL. This PORTAL remains the entry point to BSNL WiFi network and users have to authenticate on this portal. The authentication can happen using either username/password pair OR using MSISDN/OTP pair OR using E-Voucher/Scratch Card Voucher OR using MAC based authentication depending on use case which is running on that relevant SSID.

1.3 **AAA Server:** Authentication parameter/credentials reach this AAA Server from CAPTIVE PORTAL OR from Mobile APP. For BSNL existing packet core users this AAA server performs authentication from BSNL HLR depending on whether the user shall be provided WiFi access or not. For BSNL existing wire line broadband users this AAA server performs authentication from BSNL Wireline network AAA server depending on whether the user shall be provided WiFi access or not. For other users which are walking/guest users this AAA server performs authentication from WiFi SMP solution.

1.4 **Policy Manager:** Policy Manager decides policies for each user and sends the enforcement of relevant policy to Wi-Fi Access Gateway (WAG). For walk in real time users it also performs the metering for usage happening. Policy and Quota Management for BSNL existing packet core users is performed through integration with BSNL packet core PCRF and IN/OCS.

1.5 **Monetization Platform:** Solution has Captive Portal, Mobile APPs where as a part of Monetization use case advertisements are shown. Such advertisements are handled using this Monetization platform which has an integrated Advertisement Server capable of sending location based dynamic advertisements. Apart from advertisements it also enables various use cases like Hot Spot locator where it is fed with the location co-ordinates of the Access Point and hotspot and based on the same Push Notifications are sent on the Mobile APP informing end user of Hot Spot availability in particular location.

1.6 **Voucher Management System:** System generates vouchers and supports physical vouchers as well as e-vouchers. On using a voucher the user shall receive internet access equivalent to the voucher definition. Users can also create account using voucher or use it for top ups. Generation of voucher happen on criteria like Number of vouchers to generate; the amount of vouchers; the validity; the expiration time of vouchers. Vouchers remain bound with hotspot locations.

1.7 **Web Self Care Portal:** Walk in Users have access to "My Account" page which is the Web Self Care Portal. Users can see their usage details on this portal and also perform Top Ups from this portal. This shall work as interface between BSNL and Wi-Fi user. Any prospective user coming into BSNL public hotspot shall be presented a webpage portal giving details of Wi-Fi services, tariffs and procedure to subscribe to the services. The link to payment gateway and to download the APP is presented to the prospective user.

1.8 **Mobile APP:** BSNL has mobile APP available at Google Play Store for Android Devices and at APP Store for iOS devices from where users can download the APP and install on their handsets.

1.9 **Enterprise Management System (EMS)** is primarily for management of Application Servers which are deployed as part of Wi-Fi Offload & SMP platform.

2. **WiFi Access Gateway (WAG):** WAG performs Local Internet Breakout at each RPOP. It integrates with BSNL network existing BSNL IN/OCS for Wireless and Wireline and Billing Systems for Charging. BSNL existing WAG is DIAMETER based and supports DIAMETER protocol and interfaces. WAG supports admission control and QoS parameter enforcement. The WAG provides the following functions:

i) Application/protocol recognition
ii) User bandwidth management
iii) Tiered services
iv) Zero rating application
v) Enabling Application based charging
vi) The WAG recognizes the most popular web protocols/applications. It is possible to add applications/protocols in the WAG Application module, without interrupting the service.

3. **DHCP**: DHCP Server handles performing IP Address allocation for the end users and for Access Points. DHCP system allocates IP addresses dynamically to WiFi users and to the local subnet devices which require dynamic IP from the DHCP server.

4. WLC shall interface with Wi-Fi backhaul to carry traffic from hotspot location to core network AAA, WiFi Access Gateway (WAG).

5. **Detailed Scope of Field work:**

5.1 **Site Walkthrough to create RF design and generate the final design report**

i) Collection of Floor plan (Need to draw approximate floor plan if not available).
ii) Collection of structural details like type of wall material, ceiling height etc.

iii) Identify potential AP locations.
iv) Identify potential location for installation of rack, UPS, Power Supply etc.
v) Identify availability of backhaul transmission medium.
vi) Identify feasible cable route.

5.2 **Access Point Installation and Commissioning (I & C)**

i) Cabling and installation of Access Points, Racks and Switches in accordance with the Final Design Report.
ii) Procurement of other ancillaries like Pole/Mast/Pipe, Clamps, conduit for cable, rack, connectors, weather proof kit etc which would be required for installation of access points & other hotspot location equipments.
iii) Configure the Access Points and the L2 Switches as per the planning guidelines (IP Addressing and VLAN Configuration).
iv) Coordinate for integration of the Access Points through WLC to BSNL Wi-Fi core.

5.3 **Post Installation Validation and Optimization**

i) Conduct internal & external venue walk tests to collect RF data at the premise post Wi-Fi Deployment.
ii) The Walk test tool (Software and Hardware) specific to Collect Wi-Fi RF Measurements shall be arranged by the Bidder at their cost. All the Survey details have to be stored electronically at the central site of BSNL for future reference and O&M.
iii) Coordinate for performing RF Optimization activities.
iv) Perform Acceptance Testing as per the Acceptance Test Plan provided to them.
v) Revisits may be required during the RF optimization phase if the Acceptance Criteria are not met.

5.4 **Service provisioning and Configuration**

i) Network Provisioning - AP, WLC, and associated EMS
ii) Creation of tasks that update the configuration, reboot, or update of the firmware of a group (one or more) of access points according to a schedule
iii) Backup of AP Configuration.

5.5 **Operation and Maintenance**

i) Field Operations team for providing services for WLC, EMS & all Hotspot location equipments.
ii) The units and systems must be serviced regularly
iii) Preventive maintenance on each Site
iv) handling of the spare parts needed for carrying out Corrective, Preventive or planned maintenance activities
v) Ensures End-2-End delivery of WI-FI Solution all the time as per SLA.
vi) Performs all activities related to Optimization required for WI-FI Solution as per KPIs and SLAs defined.
vii) UPS Maintenance

5.6 **Fault Management**

i) Manages alarms and problems for WI-FI services on 24 X 7 basis.
ii) Maintains availability of Wi-Fi services through resolving problems and performance
iii) Field Visit of AP for fault management, Preventive Maintenance, Software upgradation etc.

5.7 **Service Level Agreement and Penalties.**

5.7.1 **Delayed Commissioning:** The commissioning of total network/site including supply of the equipment is to be completed as per agreement/Work Order from the date of signing/receipt of agreement/Work Order to PWP. A penalty at the rate of 0.5% of the cost of hardware/bandwidth charges of the location not completed shall be payable per week of delay or part thereof subject to a maximum of 5% for that site. If the delay is more than two weeks, then BSNL shall have the right to terminate the agreement/contract with a penalty of 5% of total work order cost and get the work done by other PWP.

1. Wi-Fi Hotspots Network Operations and Maintenance Services have to be provided on 24 × 7 bases.
2. Any other activity or equipment, which is not explicitly covered in this document but is essential, as part of the operations and Maintenance of Wi-Fi network shall also be performed by the PWP partner. In case of any dispute in this regard, decision of BSNL shall prevail.

3. PWP shall at least meet the criterion for uptime of services **(99.99 %)** and also Quality of Service benchmarks for the wireless data services.
4. The penalties shall be applicable if the failure/disruption is due to the fault on part of the PWP. PWP shall not be penalized if the failure is due to fault on account of BSNL part. Vendor shall provide SLA measurement tool for Operation & Monitoring the Wi-Fi offload solution, Central equipment & Hotspot location uptime and also the service availability Report on above SLA items shall be submitted on monthly basis.
5. **In case the customer imposes any penalty on BSNL for services deterioration/poor quality of service (QoS) or non-availability of services due to faulty Wi-Fi hotspots (vendor fault) then same shall be recoverable from PWP.**

6 Revenue share Model & Business allocation rule among partners:

6.1 As per Wi-Fi Open Policy for PWPs, the revenue share arrangement with Model-II is as below:

Model Name	Revenue Share to the PWP in enterprise/Bulk plans
Model – II	50%

6.2 To enable the business opportunity on a faster pace, following method shall be followed for Wi-Fi business allocation among partners.

a. The partners empanelled under Model-II shall be eligible to work in UP East Circle
b. Model-III empanelled partners can also be on-boarded as Model-II.

6.3 The Business acquired by BSNL on nomination basis or otherwise, the business will be allocated between the different Empanelled Partners on H1 basis (highest revenue share to BSNL). Circle/BA, who acquires the business, will call for sealed quotes/bid from empanelled Partners to offer additional revenue share to BSNL by PWP[plus percentage over and above the minimum revenue share decided by BSNL for the service as per relevant provisions in this EOI.

6.4 PWP partners will be using BSNL Wi-Fi Core for the delivery of Wi-Fi Solution to the customers. **Business lead will be allocated to the Partner offering maximum revenue share for that specific business opportunity/deal.**

6.5 Since in the revenue share model, the revenue from the customer is generally the same on year-on-year basis, the division of the work between H1 and H2 60:40); Between H1, H2 and H3 (in 50:30:20); and H1 alone shall be done as per the table below:

Sr. No.	Project Value/customer order value (for 1 year)	Work distribution Ratio H1:H2:H3	Ownership for Central Dashboard (for Wi-Fi status monitoring as asked by end customer)
1	>100 Cr	50:30:20	Partner with 50% share
2	10 – 100 Cr	70:30	Partner with 70% share
3	<10 Cr	H1 Partner	H1 Partner

7. Available Plans for Bulk/Enterprise Customers: Currently available PWP using FTTH backhaul are as below:

1. Bharat Fibre/ Bharat Air Fiber plans for Public Data office (PDO)

Plan Name	No of Aps	Bandwidth (in Mbps)	Annual Plan Charges (in Rs.)
PDO Premium	1	Up to 100 Mbps	11988 (Monthly Rs. 999)

2. Plans for enterprise customers.

Plan Name	No. of APs	Bandwidth	Annual Plan Charges (in Rs.)
PWP 210	1 to 2	10	200000
PWP 410	3 to 4	10	250000
PWP 420	3 to 4	20	300000
PWP 730	5 to 7	30	480000
PWP 1040	8 to 10	40	550000
PWP 1450	11 to 14	50	800000
PWP 1760	15 to 17	60	925000
PWP 2080	18 to 20	80	1025000

3. Economical PWP FTTH Plans for enterprise customer.

Plan Name	**No of Aps**	**Bandwidth (in Mbps)**	**Annual Plan Charges (in Rs.)**
EPWP110	1	10	49999
EPWP120	1	20	59999
EPWP220	2	20	79999
EPWP250	2	50	99999

PART IV

SPECIAL CONDITION

1. **Certificates from all Directors/Partners/Proprietor of the bidding firm stating that none of their near relatives are working in BSNL.**

2. **Valid Goods and Service Tax (GST) registration Certificate of the bidding Firm/Company with self-declaration on company letter head that bidder is not black listed by GST authorities and in case bidder gets blacklisted by GST authorities during the tenure of contract with BSNL, bidder indemnifies BSNL from any monitory loss caused due such blacklisting i.e. Loss of input credit claim etc and ensures that such loss will be paid to BSNL by the Service provider.**

3. Bidder should not have been debarred /blacklisted in anywhere in India by BSNL/by any State/Central PSU/any State Govt. department/Central Govt. Department. Following declaration has to be submitted by the firm on Rs.10 Non judicial stamp paper.

   (I /We…….. hereby declare that my/our firm has/have not been debarred for taking part in tender anywhere in India in BSNL/any State/ Central PSU/State /central Govt.. I/ We also declared that my/our firm is not under process of debarring by any unit of BSNL. I/We am/are aware that any suppression of facts in this regard/breach of this condition/clause would result in immediate termination of contract/cancellation of the existing contract/contracts and also forfeiting of my/our security deposit held).

4. INDEMNITY: The Contractor hereby agrees and covenants to indemnify and keep indemnified BSNL against:-
   4.1 All loss, misappropriations, misuse or damage of or to the documents of any other security instruments which are in possession of the Contractor or its personnel or within the control of the Contractor or its personnel.
   4.2 Any or all claims, liabilities, damages, losses, costs, charges, expenses, proceedings and actions of any nature whatsoever made or instituted against BSNL and/ or any customer directly or indirectly by reason of.
5. UNDERTAKING & DECLARATION: PWP should submit the undertaking and declaration as per annexure:

ANNEXURE-I

DEFINITIONS OF TERMS AND EXPRESSIONS

Unless the context otherwise requires, the different terms and expression used shall have the meaning assigned to them in the following paragraph,

1. The "Wi-Fi Core" means software & hardware that offers a comprehensive solution for Subscriber Management platform, Captive Portal, Online charging system, AAA, WAG, DHCP, monetization platform etc. for providing Wi-Fi services.

2. "Wi-Fi Access Services" means hardware and software for supporting Wi-Fi Access Points, their configuration, monitoring etc.

3. "Wi-Fi Hotspots" means combination of hardware(s) such as Access Points (APs) and associated infra items such as power backup, bandwidth connectivity, racks etc.

4. "BSNL Network" means the Central networks of BSNL for providing the various landline, FTTH, GSM, Broadband etc. services to its subscribers.

5. "Validity of the agreement" is the period for which this agreement may be effective.

6. The term "Services" or "Service" means Wi-Fi services (Retail and Enterprise both) as defined in Annexure II to this Agreement, as required under the context.

7. "BSNL" means **BHARAT SANCHAR NIGAM LIMITED**.

8. "PWP" means Public Wi-Fi Partner who is to be engaged for provisioning of services.

9. "PDO" means public data offices which are Retail Hotspot locations such as retail shops may be tea/coffee/groceries where good number of foot falls is involved.

10. "Plans" means Charges payable by the subscriber for the service provided.

11. "TRAI" means Telecom Regulatory Authority of India established under the TRAI Act,

ANNEXURE-II

I. ARBITRATION (Applicable in case of supply orders/Contracts with firms, other than Public Sector Enterprise) (Not applicable in cases valuing less than Rs. 5 lakhs)

Except as otherwise provided elsewhere in the contract, if any dispute, difference, question or disagreement arises between the parties hereto or their respective representatives or assignees, in connection with construction, meaning, operation, effect, interpretation of the contract or breach thereof which parties unable to settle mutually, the same shall be referred to Arbitration as provided hereunder:

(1) A party wishing to commence arbitration proceeding shall revoke Arbitration Clause by giving 60 days' notice to the designated officer of the other party. The notice invoking arbitration shall specify all the points of disputes with details of the amount claimed to be referred to arbitration at the time of invocation of arbitration and not thereafter. If the claim is in foreign currency, the claimant shall indicate its value in Indian Rupee for the purpose of constitution of the arbitral tribunal.
(2) The number of the arbitrators and the appointing authority will be as under:

Claim amount (excluding claim for counter claim, if any)	**Number of arbitrator**	**Appointing Authority**
Above Rs. 5 lakhs to Rs. 5 crores	Sole Arbitrator to be appointed from a panel of arbitrators of BSNL.	BSNL (Note: BSNL will forward a list containing names of three empanelled arbitrators to the other party for selecting one from the list who will be appointed as sole arbitrator by BSNL)
Above Rs. 5 crores	3 Arbitrators	One arbitrator by each party and the 3rd arbitrator, who shall be the presiding arbitrator, by the two arbitrators. BSNL will appoint its arbitrator from its panel.

(3) Neither party shall appoint its serving employee as arbitrator.

4. If any of the Arbitrators so appointed dies, resigns, becomes incapacitated or withdraws for any reason from the proceedings, it shall be lawful for the concerned party/arbitrators to appoint another person in his place in the same manner as aforesaid. Such person shall proceed with the reference from the stage where his predecessor had left it both parties consent for the same; otherwise, he shall proceed de novo.

5. Parties agree that neither party shall be entitled for any pre-reference or pendent-lite interest on its claims. Parties agree that any claim for such interest made by any party shall be void.

6. Unless otherwise decided by the parties, Fast Track procedure as prescribed in Section 29 B of the Arbitration Conciliation Act, 1996 for resolution of all disputes shall be followed, where the claim amount is upto Rs. 5 crores.

***[29B. Fast track procedure** – (1) Notwithstanding anything contained in this Act, the parties to an arbitration agreement, may, at any stage either before or at the time of appointment of the arbitral tribunal, agree in writing to have their dispute resolved by fast track procedure specified in sub-section (3).*

(2) The parties to the arbitration agreement, while agreeing for resolution of dispute by fast track procedure, may agree that the arbitral tribunal shall consist of a sole arbitrator who shall be chosen by the parties.

(3) The arbitral tribunal shall follow the following procedure while conducting arbitration proceedings under sub-section (1):-

(a) The arbitral tribunal shall decide the dispute on the basis of written pleadings, documents and submissions filed by the parties without oral hearing;
(b) The arbitral tribunal shall have power to call for any further information or clarification from the parties in addition to the pleadings and documents filed by them;
(c) An oral hearing may be held only, if, all the parties make a request or if the arbitral tribunal considers it necessary to have oral hearing for clarifying certain issues;
(d) The arbitral tribunal may dispense with any technical formalities, if an oral hearing is held, and adopt such procedure as deemed appropriate for expeditious disposal of the case.

(4) The award under this section shall be made within a period of six months from the date the arbitral tribunal enters upon the reference.

(5) If the award is not made within the period specified in sub-section (4), the provisions of sub- sections (3) to (9) of Section 29 A shall apply to the proceedings.

(6) The fees payable to the arbitrator and the manner of payment of the fees shall be such as may be agreed between the arbitrator and the parties.]

7. The arbitral tribunal shall make and publish the award within time stipulated as under:

Amount of Claims and Counter Claims	Period for making and publishing of the award (counted from the date the arbitral tribunal enters upon the reference)
Upto Rs. 5 crores	Within 6 months (Fast Track procedure)
Above Rs. 5 crores	Within 12 months

However, the above time limit can be extended by the Arbitrator for reasons to be recorded in writing with the consent of parties and in terms of provisions of the Act.

8. In case of arbitral tribunal of 3 arbitrators, each party shall be responsible to make arrangements for the travel and stay, etc. of the arbitrator appointed by it. Claimant shall also be responsible for making arrangements for travel/stay arrangements for the Presiding Arbitrator and the expenses incurred shall be shared equally by the parties.

In case of sole arbitrator, BSNL shall make all necessary arrangements for his travel/stay and the expenses incurred shall be shared equally by the parties.

9. The Arbitration proceeding shall be held at New Delhi.

10.Subject to the aforesaid conditions, provisions of the Arbitration and Conciliation Act, 1996 and any statutory modifications or re-enactment thereof shall apply to the arbitration proceedings under this clause.

II. APPLICABLE LAW AND JURSDICTION

(a) The supply order for Goods 'or' Services, including all matters connected with this supply order shall be governed by the Indian law both substantive and procedural, for the time being in force and shall be subject to the exclusive jurisdiction of Indian Courts at the place from where the agreement has taken place.

(b) Foreign companies, operating in India or entering into Joint Ventures in India, shall have to obey the law of land and there shall be no compromise or excuse for the ignorance of the Indian legal system in any way.

Annexure-III

DRAFT AGREEMENT WITH REGARD TO SECURITY REQUIREMENTS

This **AGREEMENT** is made and entered into at Hazratganj, Lucknow on this the …….day of month, 2023

BY AND BETWEEN

Bharat Sanchar Nigam Limited, a company incorporated under the Companies Act, 1956 and having its registered office at 2nd Floor, Bharat Sanchar Bhawan, HC Mathur Lane, Janpath, New Delhi 110001(hereinafter referred to as "**BSNL**" or the "**TSP**", which expression shall, unless repugnant to the context or meaning thereof, include its successors and permitted assigns) of the **FIRST PART**;

AND

[●], a company incorporated under the Companies Act, 1956 and having its registered office at [●] (hereinafter referred to as the "**Supplier**" or the "**Vendor**", which expression shall, unless repugnant to the context or meaning thereof, include its successors, and permitted assigns) of the **OTHER PART**.

(BSNL/TSP and the Supplier/Vendor shall be collectively called as the "Parties" and individually a "Party".)

RECITALS

A. The Vendor has been empaneled under **OPEN POLICY FOR PUBLIC Wi-Fi PARTNERS FOR ENTERPRISE AND RETAIL SERVICES** (BSNLCO-NPBB/21(11)/1 dated 24.06.2021).

B. Pursuant to the provisions of Clause [1] of Agreement, the Parties are executing this Agreement, subject to the terms and conditions as provided hereinafter.

NOW THEREFORE, IN CONSIDERATION OF MUTUAL REPRESENTATIONS, COVENANTS AND OTHER VALUABLE CONSIDERATION, THE RECEIPT AND SUFFICIENCY OF WHICH IS HEREBY ACKNOWLEDGED, THE PARTIES HEREBY AGREE AS FOLLOWS:

1. Definition & Interpretation

1.1 Definitions

Unless the context otherwise requires, the different terms and expression used in this Agreement shall have the meaning assigned to them for the purpose of this Agreement:

“Access” shall mean the interconnection with TSP Systems or access to or use of TSP Information stored on TSP Systems through interconnection with TSP Systems or access to or use of TSP Information stored on Vendor Systems or access to or use of TSP Information stored in any mobile device.

“**Applicable Laws**” shall mean any law, statute, ordinance, rule, regulation, guideline, policy or other pronouncement having the effect of law of any Governmental Authority as interpreted and administered including any modifications or amendments thereto.

“Authorised” shall refer to the approval by TSP of the Access as part of the authorisation process and the Vendor Contact has a record of this authorisation. The term “Authorisation” shall be construed accordingly.

“Commencement Date”” shall mean the date when the Agreement is executed

“Contract Personnel” means dedicated resources of the Vendor in terms of employees, subcontractors including employees of sub-contractors and agents including agent’s sub contractors and their employees engaged for the purpose of this Agreement.

“End Date” shall have the meaning assigned to it in Clause 16.1.

“**Escrow Information”** shall have the meaning assigned to it in Clause 7.11 (a).

“**Governmental Authority**” shall mean any governmental authority, statutory authority, government department, ministry, secretariat, agency, commission, board, tribunal, court or other law, rule or regulation making body/ entity having or purporting to have jurisdiction on behalf of the Republic of India or any other government having or purporting to have jurisdiction over a Party, or any state or other subdivision thereof or any municipality, district or other subdivision thereof including, without limitation, the Chairman, Department of Telecommunications, Ministry of Communications, Government of India and/or any other telecom regulatory authority, including Telecom Engineering Center, having competent jurisdiction; and/or Chairman, Telecom Regulatory Authority of India, and includes any officer empowered by them to perform all or any of the functions of such a governmental authority.

“**Information**" shall mean technical, financial and commercial information and data relating to Party’s respective businesses, finances, planning, facilities, products, techniques and processes and shall include, but not limited to, discoveries, ideas, concepts, know-how, techniques, designs, specifications, drawings, blueprints, tracings, diagrams, models, samples, flow charts, data, computer programs, disks, diskettes, tapes, marketing plans, customer names and other technical, financial or commercial information and intellectual properties, whether in written, oral or other tangible or intangible forms.

“**Licensor**” shall mean the Department of Telecommunications, Ministry of Communications & IT, Government of India.

“Personal Data” shall comprise of customer details and Call Detail Record (CDR).

“Sensitive Information” shall mean any TSP Information marked as classified as per TSP’s data classification policy or deemed business critical. This also includes any other data, or element of information, notified as such by the Government (e.g. IT Act 2000).

“Security Standards” shall mean all the relevant contemporary standards associated with national and international security standard related to IT & Telecom equipment hardware and software and those related to information & communication security, including but without limitation to ISO 27000 series, ISO/ IEC 15408, 3GPP, 3GPP2, WiMAX etc. and as evolved from time to time.

“Subcontractor” shall mean any person, partnership or corporation with whom the Vendor places a contract and/ or an order for the supply of any equipment, item, service or for any work in relation to the purpose of this Agreement. The term "Subcontract" shall be construed accordingly.

“Supplies” shall mean all components, materials, plant, tools, test equipment, documentation, hardware firmware, software, spares parts, services and all the things & items to be provided to TSP pursuant to the Agreement together with all Information and Work the Agreement requires to be supplied or performed for TSP.

“Term” shall mean the term of this Agreement starting from the Commencement Date upto the End Date.

"TSP" shall mean Bharat Sanchar Nigam Limited who has been issued the CMTS license under section 4 of Indian Telegraph Act 1885 by the Licensor, Government of India

"TSP Group Security" shall mean the security organization based within the TSP.

"TSP Information" shall mean all data including data, text, image, sound, voice, codes, circuit diagrams, core & applications software and database, intellectual property as well as personal, public, operational and services data in TSPs custody which is and /or received which are supplied/ shared with Vendor for the purpose of this Agreement or are obtained by the Vendor on behalf of TSP.

"TSP Items" shall mean all items provided by TSP to the Vendor and all items held by the Vendor which belong to TSP.

"TSP Regulatory Contact" shall mean in-charge of TSP Regulatory Operations or such other person whose details shall be notified by TSP to the Vendor from time to time.

"TSP Security Contact" shall mean in-charge of TSP Security Operations Centre or such other person whose details shall be notified by TSP to the Vendor from time to time.

"TSP Systems" shall mean any TSP computer, application, databases, network infrastructure, network elements and appliances, core and applications software or such other systems as may be agreed in writing from time to time between TSP and the Vendor.

"Vendor" shall mean the vendor who supplies equipment, software and is and/or managed services to TSP for the purpose of installation, testing, commissioning, provision, operations and/or maintenance of TSP's networks.

"Vendor Security Contact" shall mean such person whose details shall be notified by the Vendor to TSP from time to time for such purpose.

"Vendor Regulatory Contact" shall mean such person whose details shall be notified by the Vendor to TSP from time to time for such purpose.

"Vendor Systems" shall mean any Vendor owned computer hardware or software, application database or network elements / appliance or such other systems as may be agreed in writing from time to time by TSP and the Vendor.

1.2 Interpretation

Unless otherwise stated or unless the context otherwise requires, in this Agreement:

(a) the headings, whether of Clauses or other parts of the Agreement, are for ease of reference only and shall not be relevant to interpretation;
(b) the references to the Recitals, Clauses, Schedules and Annexures shall be references to the recitals, clauses, schedules and annexures of this Agreement;
(c) words importing the singular shall include plural and vice versa;
(d) words denoting any gender shall include all genders;
(e) where a word or phrase is defined, other parts of speech and grammatical forms of that word or phrase shall have corresponding meanings;
(f) references to statutes or statutory provisions include references to any orders, or regulations made there under and references to any statute, provision, order or regulation include references to that statute, provision order or regulation as amended, modified, re-enacted or replaced from time to time whether before or after the date thereof.

2. Scope

This Agreement sets out the provisions under which the Vendor will be able to supply equipments and services and be granted Access to TSP Systems, network, equipments, data and facilities and TSP Information including Sensitive Information for the purpose of the planning, engineering, supply, installation, testing, commissioning, operations and maintenance, annual maintenance on network/equipment as per the contract.

3. International Security Standard Certification

The Vendor shall have contemporary relevant Security standard certification and shall comply with the provisions of security standards certification with respect to Telecom & IT equipment hardware and software and those related to information & communication security management, such as ISO 15408 standards as applicable to IT and IT related products, ISO 27001 for Information Security Management System, standards used by other relevant standard formulation bodies for Telecom equipment like 3GPP, 3GPP2, ITU standard etc or equivalent acceptable international standards or certification. Based on the requisite testing to be conducted at their labs, vendors will certify their own equipments as required under this clause. IT related elements in the telecom networks of the concerned OEMs, which are already ISO 15408 certified will be accepted as certified. Vendor will submit a relevant self-certificate based on test reports in this regards.

4. Security Requirements:

The Vendor shall comply with following security policies:

4.1 General

4.1.1 The Vendor shall be Authorized to access only TSP Systems and Information in accordance with the provisions of this Agreement and only during the Term of this Agreement.

4.1.2 The Vendor shall identify to the TSP, details of Vendor Security Contact at the Commencement Date who will act as a single point of contact for TSP, such as a senior manager or CIO responsible for security, for any security issues. This responsibility shall be detailed within his/her job description. Notwithstanding anything to the contrary, the Vendor shall at all times be responsible to the TSP for any security related issues. It is clarified that the Vendor Security Contact shall be a security cleared Indian national. The security clearance for the Vendor Security Contact will be applied, within one month of date of submission of necessary document by the vendor to TSP.

4.1.3 As part of the Authorization process, details of Vendor's Contract Personnel that need Access will be requested by TSP. The Vendor Security Contact shall at all times ensure that only Contract Personnel who have a need to Access in order to fulfill the purpose of this Agreement are Authorized. This Authorization and any changes in the Contract Personnel would be notified by the Vendor for the information and for the approval (wherever applicable) of the TSP.

4.1.4 Pursuant to Clause 4.1.3 above, the Vendor acknowledges that only the Contract Personnel having requisite training are Authorized to access the TSP System.

4.1.5 The Vendor shall have a well defined Information Security policy compliant with ISO/IEC 27001:2013 or have equivalent standards and in line with the TSP's information security policies and requirements.

4.1.6 The Vendor shall ensure that they have information security organization in place to implement the provisions of TSP's information security policies. The Information Security responsibilities of all Vendor employees working for TSP shall be defined and communicated.

4.1.7 The Vendor shall establish and maintain contacts with special interest groups to ensure that the understanding of the information security environment is current, including updates on security advisories, vulnerabilities and patches and ensure that the same is implemented.

4.1.8 The Vendor shall conduct a Risk Analysis and ensure that all risks due to it own and subcontractors' operations with TSP are identified, measured and mitigated as per the TSPs requirements. The Risk Assessment report is required to be shared with the Chief Security officer/CISO of TSP.

4.2 Physical Security

4.2.1 All Contract Personnel including sub-contractors and their employees, agents and their employees of the Vendor working on TSP premises shall be in possession of a TSP Identification or Electronic Access Control ("**TSP ID/EAC**") card. This card is to be used as a means of identity verification on TSP premises at all times and as such the photographic image displayed on the TSP ID/EAC card must be clear and be a true likeness of the Contract Personnel. If the TSP has any advanced identity verification systems the same would also apply. TSP and Vendor will mutually agree to re- define such verification measures from time to time

4.2.2 All Contract Personnel including sub-contractors and their employees, agents and their employees of the Vendor accessing premises (sites, buildings or internal areas) , where TSP Information is stored or processed, shall be in possession of an Identification or Electronic Access Control ("**ID/EAC**") card. This card is to be used as a means of identity verification on these premises at all times and as such the photographic image displayed on the ID/EAC card must be clear and be a true likeness of the Contract Personnel or the Subcontractor or the Vendor's employees, subcontractors and agents. If the TSP has any advanced identity verification systems the same would also apply. TSP may re-define such verification measures from time to time

4.2.3 The Vendor shall not (and, where relevant, shall procure that any Contract Personnel shall not) without the prior written Authorization of the TSP Security Contact connect any equipment, device or software to any TSP System and where it is not intended to be connected at a point in the TSP system.

4.2.4 The Vendor shall be able to demonstrate that it has procedures to deal with security threats directed against TSP or against a Vendor working on behalf of TSP whilst safeguarding TSP Information.

4.2.5 The Vendor and/or its Contract Personnel shall not access TSP's electronic systems without first obtaining the written consent of the TSP Security Contact.

4.2.6 The Vendor's Access to sites, buildings or internal areas where TSP Information is stored or processed, shall be as Authorized and the Vendor and all its Authorized personnel shall adhere to robust processes and procedures to ensure compliance.

4.2.7 The Vendor shall not conduct recording, photography or video graphic at TSP premises that captures any TSP Information, without prior authorization from the TSP Security Contact.

4.2.8 If already available at the TSP Premises, CCTV security systems and their associated recording medium shall be used by the TSP/Vendor either in response to security incidents, as a security surveillance tool, as a deterrent or as an aid to the possible apprehension of individuals caught in the act of committing a crime. As such, these systems shall be Authorized by appropriate TSP Security Contact when used by Vendor.

4.2.9 The Vendor shall maintain a controlled record of all assigned TSP physical assets and assigned TSP Items to them.

4.2.10 The local area surrounding the Vendor’s facilities at TSPs premises over which Vendor has authorized control shall be physically inspected for security risks and threats by the Vendor in case of any abnormal activity / incident found / observed shall report the same to TSP.

4.2.11 The Vendor shall disable the Access immediately if any Contract Personnel is no longer require Access or has changed roles for any reason whatsoever or whose integrity is suspected or considered doubtful or as may be notified by TSP in accordance with clause 4.3.1.

4.3 Logical Security

4.3.1 The Vendor shall notify TSP immediately if any Contract Personnel no longer requires Access or changes role for any reason whatsoever thus enabling TSP to disable or modify the Access rights.

4.3.2 The Parties shall, implement agreed security measures across all supplied components and materials including software & data to ensure safeguard and confidentiality, availability and integrity of TSP Systems and TSP Information, Parties shall prepare documentation in relation to the implementation of logical security and shall ensure that it has such security as:

(a) prevents unauthorized individuals e.g. hackers from gaining Access to TSP Systems; and
(b) reduces the risk of misuse of TSP Systems or TSP information, which could potentially cause loss of revenue or service (and its Quality) or reputation, breach of security by those individuals who are Authorized to Access it; and
(c) detects any security breaches that do occur enabling quick rectification of any problems that result and identification of the individuals who obtained Access and determination of how they obtained it.

4.4 Information Security

4.4.1 The Vendor shall not use TSP Information for any purpose other than for the purposes for which they were provided to the Vendor by TSP and only to the extent necessary to enable the Vendor to perform as per this Agreement.

4.4.2 The Vendor shall ensure that all information security requirements in this Agreement are communicated including in writing to all Contract Personnel in relation to their role.

4.4.3 The Vendor shall ensure procedures and controls are in place to protect the exchange of information through the use of emails, voice, facsimile and video communications facilities.

4.5 Contract Personnel Security

4.5.1 The Vendor shall ensure that the TSP Information provided under this Agreement is used only to the extent necessary to enable the Vendor to perform its obligations as per the terms of this Agreement. All Contract Personnel shall sign a confidentiality agreement either as part of their initial terms and conditions of employment or when they start working in TSP buildings or on TSP Systems and TSP Information. These confidentiality agreements shall be retained by the Vendor and shall be made accessible to TSP, if required.

4.5.2 The Vendor shall deal with breaches of security policies and procedures, including interfering with or otherwise compromising security measures, through a formal disciplinary process.

4.5.3 The Vendor shall provide a 'whistle blower' facility, available to all staff, with all TSP related issues reported back to the TSP Security Contact to the extent permissible by the law in a location in India where the Vendor is providing the services. . For the avoidance of doubt, this facility shall be used by the Contract Personnel if TSP’s employee, agent or contractor instructs Contract Personnel to act in an inconsistent manner in violation of the Agreement.

4.5.4 The Vendor shall ensure that in respect to any Contract Personnel assigned to this Agreement, it shall carry out recruitment checks in accordance with its policies.

4.5.5 The Vendor shall ensure that all Contract Personnel maintain a clear-desk and a clear screen policy to protect TSP Information, as per internal policy.

4.5.6 The Vendor shall ensure that an auditable process is developed for the ongoing control and management of Contract Personnel access profiles.

4.5.7 The Vendor shall, and shall procure that if a Contract Personnel’s job or role has been changed or terminated, such Contract Personnel shall securely destroy any TSP Information received in a recorded form from TSP (or has recorded received TSP Information) in accordance with its internal policy. Vendor may retain one copy of such information for archival policy provided it does so in a secure manner..

4.5.8 The vendor may perform the above activities as per its internal policy, which shall be shared with BSNL from time to time.

4.6 Additional Security Policies

4.6.1 The Vendor shall have documented operating procedures to discharge the security requirements detailed within this Agreement and provide TSP with access to such documentation in accordance with “Access to Vendor systems” as stipulated in this Agreement.

4.6.2 The Vendor shall implement a controlled exit procedure in respect of the individual Contract Personnel to ensure the return of any TSP assets or TSP Items or TSP Information in the possession of the individual when any of the Contract Personnel who have Access, leave the employment of the Vendor or are no longer engaged for the purpose of this Agreement. Such controlled exit procedure shall include a written communication by the Vendor Security Contact to TSP Security Contact of this removal.

4.6.3 The Vendor shall inform the TSP Security Contact immediately upon its becoming aware of any actual or suspected unauthorized Access or misuse of TSP Systems or TSP Information or breach of any of the Vendor's obligations under this Agreement.

4.6.4 The Vendor shall maintain integrity of the software build including upgrades, operating systems and applications from factory to desk. The Vendor shall demonstrate that the software build (both proprietary and off-the-shelf) delivered to TSP is the same as the software build agreed with TSP. The software as provided by Vendor should not have any known viruses or malware which could hamper security including any unauthorized leakage of TSP Information including Sensitive Information.

4.6.5 Any change of location by the Contract Personnel or Vendors support centers shall be notified to TSP.

4.6.6 Where Vendor uses subcontractors,, TSP may require that the associated security risks are clearly identified and assessed by TSP Group Security or the appropriate TSP line of business security team. This will ensure that any unacceptable security risks are identified and addressed. This in anyway shall not reduce the Vendor from being responsible to TSP for its obligations to be performed under this Agreement relating to security.

4.6.7 Where Vendor uses subcontractors, formal contracts containing all necessary security requirements shall be put in place between the Vendor and its subcontractor before the Subcontractor or its personnel can access TSP Systems and TSP Information or occupy space in TSP’s buildings or space in the Vendor’s building that is used to access, hold or process TSP Information.

4.6.8 TSP may update from time to time, security related policies, guidelines, standards and requirements. TSP will incorporate such updates by reference which shall be notified in writing by TSP to the Vendor promptly. If the Vendor has an issue with such updates, the Vendor shall promptly detail its concerns to TSP in writing.

4.6.9 The Vendor shall record and maintain detailed information of all Contract Personnel who are authorized to Access TSP Systems or TSP Information.

5. Access to TSP Systems

5.1 Subject to the provisions of this Agreement, the TSP allows (so far as it can and is able to do so) the Vendor, to have Access solely for the purpose as contemplated herein during the Term of this Agreement.

5.2 In relation to Access, the Vendor shall (and, where relevant, shall procure that all Contract Personnel shall):

a) Ensure each individual Contract Personnel has a unique user identification and password known only to such user for his/her sole use.

b) Ensure Contract Personnel never share user identification, passwords or security tokens.

c) Promptly provide to TSP such agreed reports as TSP shall from time to time require concerning the Vendor’s use and security of Access and any related matters to Access.

d) Ensure onward bridging or linking to TSP Systems is prevented unless authorized by TSP.

e) Use all reasonable endeavors to ensure no viruses or malicious code like malware, spyware, key logger, bots (as the expressions are generally understood in the computing industry) are introduced, and that there is no corruption or modification or compromisation of TSP Systems or TSP Information, while meeting out the obligations under the Contract.

f) Use reasonable endeavors to ensure that personal files which contain information, data or media with no relevance to the purpose, are not stored on TSP building servers or TSP centralized storage facilities or TSP Systems.

5.3 If TSP has provided the Vendor with Access to the Internet/Intranet, the Vendor shall, and shall ensure that the Contract Personnel, access the Internet/Intranet appropriately. It is the Vendor’s responsibility to ensure that practical guidance on internet and email abuse (as amended) is communicated to the Contract Personnel from time to time.

5.4 The Vendor shall ensure that all Contract Personnel, subject to the Clauses headed

“Regulatory Matters” and “Confidentiality” comply with classifying and handling of Information

5.5 Any security software procured by the Vendor shall be used by the Vendor without modification, unless there is an essential need to do so, in which case appropriate controls shall be applied and the agreement of TSP Group Security sought.

6. Access to Vendor Systems

6.1 If Contract Personnel is granted Access to Vendor Systems having bearing on TSP data, information or network, the Vendor shall:

a) Ensure each individual has a unique user identification and password known only to such individual for his/ her sole use.

b) promptly provide to TSP such reports as TSP shall from time to time require, concerning the Vendor’s use and security of access to Vendor Systems.

c) Allow Access only to the minimum extent required to enable the Contract Personnel perform their duties.

d) Allow Access using a secure login process.

e) Establish and implement formal procedures to control the allocation and de-allocation of Access rights.

f) Ensure that the allocation and use of enhanced privileges and access to sensitive tools and facilities in Vendor Systems are controlled and limited to only those users who have a business need.

g) Ensure that the allocation of user passwords to Vendor Systems that hold or access TSP Information is controlled through a formal auditable management process.

h) Provide processes to demonstrate that remote and home working activities are only permitted where Authorized by TSP and subject to appropriate security controls within the Vendor’s organization including but not limited to remote Access by users being subject to strong authentication.

i) Demonstrate that users follow security best practice in the management of their passwords.

j) Implement a password management system which provides a secure and effective interactive facility that ensures quality passwords.

k) Ensure that user sessions are terminated after a defined period of inactivity.

l) Ensure that audit logs are generated to record user activity and security-relevant events and securely managed and retained with nil ability on the part of the Vendor to allow any un-authorized access or amendment to the audit logs. Such audit logs must be maintained for future reference for a period of at least one year.

m) Ensure that monitoring of audit and event logs and analysis reports for anomalous behavior and/or attempted unauthorized access are performed by Vendor’s staff independent of those users being monitored.

n) make available audit logs where required by TSP for review.

o) Ensure all systems holding, processing or accessing TSP Information shall be hardened as per industry standards.

p) Ensure that to the extent possible, development, test and live environments are segregated from each other and the other work areas in Vendor buildings.

q) Implement controls to detect and protect against malicious software and ensure that appropriate user awareness procedures are implemented.

r) Ensure that Vendor has in relation to all Vendor Systems formal security incident management procedures with defined responsibilities.

s) Ensure that any unauthorised software is identified and removed from Vendor Systems holding, processing or accessing TSP Information.

t) Ensure that Access to diagnostic and management ports as well as diagnostic tools are securely controlled to TSP's reasonable satisfaction.

u) Ensure that Access to Vendor's audit tools shall be restricted to Relevant Contract Personnel and their use is monitored.

v) Ensure that data gathered after running audit tool is properly protected.

w) Perform enhanced independent code reviews (including penetration testing) on all Vendor Systems, as a part of the Vendor's security development lifecycle (SDL).

6.2 The devices which use proprietary encryption technique should not be used for holding TSP information.

6.3 To the extent the servers are used to fulfill the purpose of this Agreement, Vendor's servers shall not be deployed on un-trusted networks without appropriate security controls.

6.4 Changes to individual Vendor Systems shall be controlled and subject to formal change control procedures. All documentation relating to Vendor Systems shall be protected from unauthorized Access or amendment.

6.5 Security procedures and controls shall be used to secure equipment holding, accessing or processing TSP Information in Vendor Systems.

7. Conditions for Equipment Vendors

7.1 Conformance to Security Standards and Policies

The Vendor shall ensure and certify that the supplied equipment has been subjected to penetration testing and all addressable vulnerabilities have been mitigated and the equipment is 'Safe to Connect' in the Telecom Network as per the latest standards and recommendations on the subject from ITU/ISO/IETF/IEC etc. It will also include that the equipment confirms to the security policies of the TSP with respect to network elements. This applies to all telecom network elements and IT equipment used in the network

The Vendor shall also ensure that the equipment supplied has all the contemporary security related features, facilities, hardware, software etc for the purpose of Interception, Monitoring, Analysis etc for use by the law enforcement agencies and provide complete information to enable these features and facilities before the supply of the equipment or the procedure of enabling these, if these are to be enabled after the commissioning of the network. The Vendor shall also submit a test report on these features and facilities and also a certificate that all contemporary features and facilities of this category exist in the equipment supplied.

Vendors will be allowed to certify their own equipments based on the testing at the labs which are capable of such testings. IT related elements in the telecom networks which are already ISO 15408 certified will be accepted as certified. Vendor can submit a relevant Self certificate based on test reports in this regard.

7.2 Equipments Configuration Guide

Two sets of equipment configuration guide should be supplied which detail the configuration required to meet the policies and standards at least in respect of following:

Network Element security policies:
- Generic OS
- Technical Standard for Switches and Routers
- Management Standard for Switches and Routers

7.3 Report

A report on the susceptibility to the attacks on mobile networks shall be provided by the Vendor to the TSP in the following manner:

(a) Next Generation Network Equipment are susceptible to several attacks. The Vendor must submit a report categorically stating that the attacks to which the equipment and the network is susceptible, the degree of risk of each type of attack and mitigation technique to deal with these attacks.. The Vendor will ensure that whatever mitigation was possible as per the current available technologies, techniques, configuration have already been used and adopted by them before the supply of the equipment.

7.4 Security from Malware

There are no known cases of malware disrupting telecom services, yet. However, malware can cause information leaks and can result in the leak of private user information. However, some viruses, worms and Trojans can infect devices and spread malware via text messages or Bluetooth connectivity. This network-based service will also block Denial of Service attacks and restrict network traffic based on source, destination, IP ports and applications. It will also allow enterprise IT managers to lock and/or delete data on lost or stolen devices. The connectivity could affect platforms if adequate firewalls, IDPs are not strong. Therefore Vendors would provide adequate firewall and IDPs with the supply of equipment.

7.5 Cryptography Related Security Issues:

Vendors will take suitable measures to deal with cryptography related vulnerabilities and submit a report of the measures along with a relevant certificate(s)that they have taken adequate measures to deal with these vulnerabilities.

i. Attacks on COMP-128 algorithm
ii. Compromised cipher key
iii. Key recovery allowing SIM cloning
iv. Hijacking outgoing calls in networks with encryption disabled
v. Hijacking outgoing calls in networks with encryption enabled
vi. Hijacking incoming calls in networks with encryption disabled
vii. Hijacking incoming calls in networks with encryption enabled
viii. Suppressing encryption between the target user and the intruder
ix. Suppressing encryption between target user and the true network

7.6 Data flow Attacks

Many sophisticated attacks disguise themselves in data flows across sessions and ports—the more traffic there is, the harder it is to identify the threats. Vendors may ensure that they are aware of this and submit compliance on the same.

7.7 Additional Interfaces

Many of the problems in the data intensive infrastructure may come to increased number of interfaces additionally for data than those were present for voice only PSTN, hence, the Vendors must give special attention to interfaces and their related vulnerability. Such Vendors may ensure that they provide additional notes that they have taken care of the same and the test mechanism and methodology adopted by them with adequate evidence.

7.8 Security against Remote Access

The Vendor shall submit a written undertaking to the TSP clearly identifying all possible means of remote control/ remote access/remote command and control in the supplied equipment as well as suitable mitigation means to close such access mechanisms.

7.9 Software and Hardware Design Surety: Vendor may choose one of the following Options for Software and Hardware Design Surety

7.9.1 Option 1:

(a) The Vendor shall at TSP's request enter into an escrow deposit arrangement in respect of all Information and documentation in relation to Supplies in respect of Hardware, executable Software/source code/gold build etc, High Level Designs (HLD), Detail Design Documents (DDD), listings and programmer's notes) ("the **Escrow Information**") as would enable TSP to complete any outstanding obligations of the Vendor under this Agreement, including, without limitation, obligations that would have existed (including the requirement to fulfil any orders that TSP would have otherwise placed under this Agreement) had this Agreement not been terminated by TSP before the expiry of its Term.

(b) Without affecting any other rights it may have, TSP shall have the right, free of charge, to use the Escrow Information, after its release, in order to use or maintain (including to upgrade) the software, to modify or have modified the software, and to authorize such modified software to or have it maintained by third parties, in case Vendor refuses to do so as per the Agreement.

(c) The Vendor shall ensure that the Escrow Information deposited in accordance with Clause 7.11 (a) is and will be maintained as sufficient to allow a reasonably skilled programmer or analyst to maintain, modify and correct the hardware and software without the help of any other person or reference, and the Vendor further undertakes to keep the Escrow Information fully upto-date throughout the Term.

(d) On the occurrence of any event permitting the release of the Escrow Information, the Vendor shall immediately provide, at its cost and expense, to TSP for a reasonable period, such advice, support assistance, data, information, access to Vendor's personnel or any key personnel of legal owner of the [Hardware and/or] Software for the purpose of understanding, maintaining (including upgrading), modifying and correcting any of the Hardware and/or Software. The softwares and codes written only in English language shall be acceptable. The code/software's shall be proven to be operational and correct version and to be certified that it does not have self-destructing programmes. This may be ensured by using the same at least once for loading the system initially before being deposited.

7.9.2 Alternative to option 1 is Option 2 as below::

(i) Gold software copy or the Executable copy of the software at the discretion of vendor.

(ii) Dumb hardware can be loaded with software by the TSP or under the supervision of TSP from Gold software copy or from the executable copy after checking that hardware is free from any software and ensuring that there are no harmful malware into the hardware. Alternatively, vendors will submit a certificate to BSNL that the supplied hardware is free from harmful malware based on the above test.

(iii) Upgradation of software for a period of as agreed in the Contract .

(iv) Design of network (network diagram of Vendor Implemented equipment under the Contract) in digital form and/ or in hard copy

7.10 Inspection

The Vendor must allow the TSP , Licensor/DoT and/or its designated agencies to inspect the hardware, software, design, development, manufacturing facility and supply chain and subject all software to a security/threat check at the time of procurement of equipment and upto two more times every year until the supplies under the Contract have been completed, at the sole discretion of the TSP. All the documents should be in English and handed over to the visiting team of the TSP at least 4 weeks ahead of the visit.

7.11 Language of Supplies

All the software codes, firmware, operating system, hardware details should be in **English** only.

8. Data Protection

8.1 The Parties acknowledge that, in respect of all personal data and processed by the Vendor for the purpose of the provision of supplies under the Contract, TSP alone as data controller shall determine the purposes for which and the manner in which such personal data will be processed by the Vendor.

8.2 Other than at TSP's request, or where required by law to provide the supplies, the Vendor shall not disclose or allow access to any Personal Data other than, subject to Clause 8.4(f) to a person placed by the Vendor under the same obligations as contained in this clause who is employed or engaged by the Vendor or within the control of the Vendor in the performance of the Agreement.

8.3 The Vendor shall not use personal data for any purpose other than the provision of the supplies and shall return any personal data to TSP immediately upon request at any time providing such return does not prevent the Vendor from fulfilling its obligations under this Agreement. The Vendor shall retain personal data no longer than is necessary for the provision of the supplies, in accordance with the relevant Applicable Law and such instructions as TSP may provide from time to time. Upon expiry or termination of this Agreement for whatever reason, the Vendor shall immediately return to TSP all personal data and certify that no copies have been made or retained by the Vendor or any third party acting on its behalf.

8.4 The Vendor shall:

(a) process personal data only on the instructions of TSP and to the extent necessary for the performance of this Agreement;

(b) not modify, amend or alter the contents of the personal data except as required or permitted by this Agreement or with TSP's prior written consent;

(c) implement the appropriate technical and organizational measures to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorized disclosure or access, and against all other unlawful forms of processing, which measures are set out in more detail in Clause 4 and provide to TSP with a written description of the measures taken when requested by TSP;

(d) comply with all relevant provisions of any TSP codes of practice notified to the Vendor from time to time and the Applicable Law ;

(e) keep all personal data secure and confidential, act only on TSP's instructions with respect to it, and comply with such further reasonable requirements from time to time of TSP for the security of it;

(f) ensure that, of the Vendor's staff, only those of the Contract Personnel who need to have access to the personal data are granted access to the personal data only for the purposes of the performance of this Agreement and the Contract Personnel are informed of the confidential nature of the personal data and comply with the obligations set out in this Clause 8;

(g) notify TSP forthwith, and in any event, no later than 12 hours from the time it comes to the Vendor's attention, that personal data transferred by TSP to the Vendor has been the subject of accidental or unlawful destruction or accidental loss, alteration, unauthorized disclosure or access, or any other unlawful forms of processing; and

(h) notify TSP in the event that it receives a request or notice from any person subject to having access to that person's personal data held by it and will provide TSP with full co-operation and assistance in relation to any complaint or request including providing TSP with any relevant personal data it holds within the timescales provided by the request or notice or as otherwise required by TSP.

8.5 In respect of transfer of personal data the following conditions shall apply:

(a) obtain TSP's prior written consent before transferring personal data to any Subcontractors in connection with the provision of the supplies;

(b) prior to any transfer of personal data, enter into or procure that any Subcontractor delivering the supplies will enter into contracts for the transfer of personal data. In respect of personal data transferred by TSP to the Vendor or acquired by the Vendor from TSP's systems to a country outside of India shall be on the basis of Applicable Laws , or such other data protection model contract terms as may be agreed between the Parties from time to time, except where the relevant Applicable Laws provides for a derogation from this requirement.

8.6 Any breach of this Clause 8 by the Vendor shall be deemed to be a material breach of the Agreement and the Vendor shall indemnify TSP from the against any costs, losses, damages, proceedings, claims, expenses or demands incurred or suffered by TSP which arise as a result of such breach.

8.7 The Vendor shall, upon TSP giving reasonable notice, allow TSP or its nominated representatives such access to its premises, Information and records and those of its agents subsidiaries and sub contractors, as may be reasonably required by TSP from time to time to assess the Vendor's and/or Contract Personnel's compliance with this Clause 8.

9. Regulatory Matters

9.1 The Vendor shall

(a) comply with all regulatory matters under Applicable Laws including, without limitation, any actions that TSP may require in connection with any regulatory matter, that are notified to the Vendor Regulatory Contact from time to time by the TSP Regulatory Contact in so far as they relate to the performance by the Vendor under the Agreement.

(b) within 14 days of the Commencement Date, ensure that the Vendor Regulatory Contact contacts the TSP Regulatory Contact to establish the nature and extent of communication between them, to assist them in meeting all regulatory requirement relevant to the Contract, as set by the Licensor or any Governmental Authority or any other person nominated by Licensor

(c) ensure that the Vendor and its Contract Personnel have undergone the proper and adequate training for the purpose of performing its obligations under this Agreement and promptly provide such information to TSP as shall be necessary for TSP to respond fully and to the timescale required to any request or requirement for information from any Governmental Authority, to the extent that such information relates to the performance of the obligations by the Vendor under the Agreement.

10. Confidentiality

10.1 In this Clause, "**TSP Information**" which TSP from time to time identifies to the Vendor as being commercially confidential, or is by its nature commercially confidential or defined by TSP as confidential, or confidential as per the Applicable Law. The term "**Information**" shall mean and include all or any communication(s), Information(s) or data disclosed, whether written, visual or oral and other material supplied to or obtained by the Party ("**Recipient**") from the other Party ("**Disclosing Party**") during the course of the Agreement.

10.2 Except with TSP's consent, the Vendor shall not disclose TSP Information to any TSP employee, not authorized to receive such information

10.3 Subject to the Clause 11, either Party receiving Information from the other shall not without the other’s prior written consent use such Information except for Contract purposes or disclose such Information to any person other than TSP's employees, agents and contractors or Contract Personnel who have a need to know and who are bound by equivalent obligations of confidentiality. Any breach of such obligations by Contract Personnel or TSP's employees, agents or contractors (as the case may be) shall be deemed to be a breach by the Vendor or TSP respectively.

10.4 Clause 10.2 and Clause 10.3 shall not apply to Information that is:

(a) published except by a breach of the Contract; or

(b) lawfully known to the Recipient at the time of disclosure and is not subject to any obligations of confidentiality; or

(c) lawfully disclosed to the Recipient by a Vendor without any obligations of confidentiality; or

(d) replicated by development independently carried out by or for the Recipient by an employee or other person without access to or knowledge of the Information.

10.5 The Vendor shall not publicize this Agreement without TSP’s prior written consent and shall ensure that any subcontractor is bound by similar confidentiality terms to those in this clause.

10.6 Either Party that has during the course of this Agreement received Information in a recorded form from the other (or has recorded received Information) shall return or destroy in a complete irrecoverable mode (at the option of the disclosing party) such records upon:

(a) expiry or termination of this Agreement; or

(b) upon earlier request unless such records are part of the supplies.

10.7 This clause shall survive termination / expiry of this Agreement.

10.8 The obligations of confidentiality shall also be governed by the Non-Disclosure Agreement dated [●] (“**NDA**”), entered into between the TSP and the Vendor. In the event of any conflict between this Clause 10 and the NDA, the provisions of the NDA shall be applicable.

11. Intellectual Property

11.1 Each Party will retain its right, title and interest in its respective trademarks, service marks and trade names as well as rights in respect of any patent, copyright, trade secrets or other intellectual property used during the performance of this Agreement. Both Parties recognize that except as otherwise expressly provided herein or agreed between the Parties, they shall have no right, title, interest or claim over the others’ intellectual property.

11.2 The Vendor agrees that it shall defend, at its own expense, all proceedings, suits and claims against and/or affecting the TSP or any of their officers, directors or employees (“Indemnitees”) with respect to infringement, breach or violation of any patent, trademark, copyright, trade secret, mark or other intellectual property rights of any third party in the course of performance of its obligations under this Agreement. The Vendor agrees that it shall indemnify the Indemnitees for all sums, costs, expenses and liabilities including, without limitation, all reasonable attorneys’ fees and other costs, incurred by Indemnities in connection with or otherwise arising out of any such proceeding, suit or claim.

If in any such suit so defended, all or any part of the equipment or any component thereof or the use thereof is held to constitute an infringement or violation of third party intellectual property rights and its use is enjoined, or if in respect of any claim of infringement or violation the Vendor deems it advisable to do so, the Vendor shall at its sole cost and expense take one or more of the following actions: (a) procure the right to continue the use of the same without interruption for the TSP; or (b) replace the same with non-infringing Equipment that meets the technical specifications stipulated under the Contract; or (c) modify the said equipment or any component thereof so as to be non-infringing; provided, that (i) the equipment or any component thereof as modified complies with all of the technical specifications as stipulated under the Contract; and (ii) Vendor shall fully indemnify the TSP for any costs associated with any such action.

12. Security Review-The Vendor shall:

a) give to (or procure the giving to) TSP (or any person authorized by TSP) such access at all reasonable times to the Vendor’s and any Subcontractor’s records and premises related to this Agreement as TSP may require from time to time to assess the Vendor’s compliance of these policies in this Agreement;

b) such assessments may include assessments of all elements of physical and logical audits, penetration testing of the Vendor’s Systems. The Vendor shall facilitate this assessment by permitting TSP to collect, retain and analyses information to identify potential security risks including trace files, statistics, network addresses and the actual information or screens accessed or transferred; and

c) provide such reports to TSP and attend such meetings as may be reasonably required by TSP.

13. Network Audit, Test and Certification:

The process of networks audit and certification should be performed by the test and certification agencies to include following activities:

(a) **Network forensics** to identify existing unwanted running processes\ malwares\ backdoors etc. on all networks' elements. The operation includes sniffing of live traffic to identify unwanted redirection and interception of traffic.

(b) **Network Hardening** to map all networks elements and to calibrate them to optimized secured state.

(c) **Network penetration test** to assure system durability against any kind of attack.

(d) **Risk assessment** to understand what actions should be taken to minimize future damage to carrier and what risks are inevitable.

(e) **Actions** to fix found problems by setting systems to default or acquiring relevant IT security technologies to prevent such problems from reoccurring.

An available list of Test and Certification Agencies (Third Parties) in various countries who may take up the regular Technical Audit of Networks and Security Certification is given at Appendix I. The TSP may engage the services of any other Network Audit and Security Certification agency also

14 Investigation:

14.1 If TSP believes that there has been a breach by the Vendor of the provisions of this Agreement, TSP will inform the Vendor Security Contact. The Vendor shall cooperate with TSP fully in any ensuing investigation. The Vendor shall provide list of users who have had access to TSP Systems and TSP Information to TSP and/or any law enforcement agency. TSP shall have access to the Vendor Systems and TSP Information in the Vendor’s premises generally with prior notice but include the right to make unannounced visits.

14.2 The Vendor shall report to TSP Security Contact promptly of any potential misuse of TSP Information or improper or unauthorized access to TSP Systems and TSP Information. Upon request, the Vendor shall promptly provide to TSP a written report with details of the potential misuse of TSP Information or improper or unauthorized access to TSP Systems and TSP Information, a remedial plan and a timetable for achievement of the planned improvements and steps to be taken to avoid the repeat of the potential misuse of TSP Information or improper or unauthorized access to TSP Systems and TSP Information.

14.3 If any audit or investigation reveals that there is a potential risk to the confidentiality, integrity or availability of TSP Information in the Vendor’s processes or Vendor Systems, Vendor shall promptly correct any security risk in the Vendor’s processes or Vendor Systems promptly.

14.4 During investigation, the Vendor shall co-operate with TSP, providing reasonable access, accommodation, facilities and assistance to all Vendor Systems as reasonably necessary to investigate the breach of the provisions of this Agreement including permitting interview of any sales, engineering or other operational personnel of Vendor. TSP shall, or at TSP’s request shall instruct the Vendor to, confiscate for evaluation any tangible or intangible asset suspected to have been used for information/ security breach or provide lead to investigation belonging to the Vendor or its subcontractor to aid the investigation.

15. Limitation of Liability

The aggregate liability of the Vendor to the TSP in respect of any breach of obligations under this Agreement shall not exceed the sum of Rs. 50,00,00,000 (Rupees Fifty Crores only) per breach, provided that such limitation shall not apply to claims arising pursuant to Clauses 10 and Clause 11.2 or pursuant to any other Clause where such limitation is expressly excluded.

16. Term and Termination

16.1 This Agreement shall be effective from the Commencement Date .Notwithstanding anything contained herein or in the Contract, this Agreement shall survive till any equipment is working, which is supplied and served by the Vendor under this Contract or for a period of ten years after signing of this Agreement whichever is later (“**End Date**”).

16.2 This Agreement may also be terminated in the event it is so determined by the Licensor or under Applicable Laws.

16.3 The termination of this Agreement shall be without prejudice to the rights and obligations of the parties which have accrued up to the date of termination.

17. Indemnity

17.1 The Vendor shall indemnify and hold harmless the TSP and its employees, agents, shareholders, directors, representatives, against any claims or penalty or consequence arising out of breach of the security related terms of the license granted by the Licensor as a result of breach or non-compliance by the Vendor with its obligations in this Agreement.

17.2 It is clarified that any expenditure incurred by the TSP for complying with security related provisions as prescribed under Applicable Law shall be borne by the Vendor. In the event there is a breach of the security related provisions as prescribed under Applicable Laws, any penalty imposed by the DoT on the TSP shall be paid by the Vendor to the TSP. Further, any testing of Vendor's equipment including requirement of testing equipment shall be met by Vendor at his own cost

18. Governing Law

This Agreement shall be governed by laws of India and the Parties agree to the exclusive jurisdiction of the Indian courts where the registered office of the TSP is situated.

20 Notices

20.1 Any notice, documents, information, direction and any other communications required or permitted to be (or such other addresses as specified in writing by the respective Party from time to time) hereunder shall be sent in writing and sent by registered post, courier and or by facsimile transmission or delivered personally by hand or sent by email addressed to the other Party to the relevant addresses set out below at the following addresses:

If to the TSP:

Chief General Manager
Bharat Sanchar Nigam Limited
CPMG Building,Hazratganj,Lucknow-226001
HC Mathur Lane
New Delhi 110001
Attention: [●]
Fax: [●]

Email: [●]

If to the Vendor:
[Name]
[Address}
Attention: [●]
Fax: [●]
Email: [●]

20.2 Any such notices and other documents shall:

(a) if delivered by hand, be deemed to have been given and received at the place of receipt on the date of delivery;
(b) if mailed by post or couriered, be deemed to have been given and received at the place of delivery on the date of delivery.
(c) if given by facsimile transmission be deemed to have been given and received, at the place of receipt on the date as shown in the facsimile transmission report; and
(d) if given by e-mail be deemed to have been given and received at the place mentioned in Clause 19 above on the same day.

20.3 Either Party shall inform the other of any change in its address above through a notice in writing to the other Party in the manner set forth above.

21. The NIT (Notice inviting tender), EoI documents (Qualifying,Financial,Technical & Commercial), letter of intent annexed hereto and such other additional particulars, instructions, drawings, work orders as may be found requisite to be given during execution of the work shall be deemed and taken to be an integral part of the contact and shall also be deemed to be included in the expression. "The Agreement" or "The Contract" wherever herein used. All clarification /modifications issued by BSNL in future shall be binding and become integral part of this agreement.

IN WITNESS WHEREOF THE PARTIES HAVE CAUSED THESE PRESENTS TO BE EXECUTED ON THE DAY, MONTH AND YEAR HEREINBELOW WRITTEN TO BE EFFECTIVE FROM THE DATE FIRST MENTIONED ABOVE

SIGNED for and on behalf of Bharat Sanchar Nigam Limited	SIGNED for and on behalf of [●]
..... Signature	..... Signature
..... Name	..... Name
..... Position	..... Position
..... Witness Signature	..... Witness Signature
..... Name & Address	..... Name & Address

Annexure IV

INDEMNITY:

The Bidder hereby agrees and covenants to indemnify and keep indemnified BSNL against:-

i) All loss, misappropriations, misuse or damage of or to the documents of any other security instruments which are in possession of the Bidder/PWP or its personnel or within the control of the PWP or its personnel.

ii) Any or all claims, liabilities, damages, losses, costs, charges, expenses, proceedings and actions of any nature whatsoever made or instituted against BSNL and/ or any customer directly or indirectly by reason of.

On behalf of BSNL for _____

The parties to this agreement have set their hands on the day mentioned hereinabove.

SIGNED AND DELIVERED by the within named party

i.e. BSNL under the hands of

Shri _____

SIGNED AND DELIVERED by the within named party

i.e. (Name of Company) _____

Shri _____

Note:

1. At SSA Headquarter the officer (s) will co-ordinate for the purpose of execution of the work. The Name & designation of the officers for co-ordination will be intimated subsequently.

Annexure V

UNDERTAKING & DECLARATION

For understanding the terms & condition of EoI & Spec. of work

a) Certified that:

1. **I**/ We …… have read, understood and agree with all the terms and conditions, specifications included in the EoI documents & offer to execute the work at the rates quoted by us in the tender form.

2. If I/ We fail to enter into the agreement & commence the work in time, the EMD/ SD/PBG deposited by us will stand forfeited to the BSNL.

b) The Bidder hereby covenants and declares that:

1. All the information, Documents, Photo copies of the Documents/ Certificates enclosed along with the Bidder offer are correct.

2. If anything is found false and/or incorrect and/or reveals any suppression of fact at any time, BSNL reserves the right to debar our offer/ cancel the LOA/ Purchase/ work order if issued and forfeit the EMD/ SD/PBG Bill amount pending with BSNL. In addition, BSNL may debar the Bidder from participation in its future EoI.

3. No addition / deletion / corrections have been made in the downloaded EoI document being submitted and it is identical to the EoI document appearing on the website.

   In case of any correction/ addition/ alteration/ omission in the EoI document, the bid shall be treated as non-responsive and shall be rejected summarily

Date: ……. ……

Signature of PWP/Bidder

Place: ……. Name of PWP/Bidder ……

Along with date & Seal

Annexure VI

DECLARATION BY BIDDER ON COMPANY LETTER HEAD IN

RESPECT OF BLACKLISTING BY GST AUTHORITIES

I,……S/o /W/o of Shri ……and proprietor/Director/Partner of M/s……do hereby affirm and declare as under:

1. That I, the sole prop./partner/Director of M/s …… (Supplier) has never been debarred and/or blacklisted by any GST authority and am not having any ongoing litigation or court cases pending or any other suite related to GST.
2. In case the above declaration is found to be incorrect or wrong, the contract if awarded to the Supplier shall be terminated immediately and the Supplier shall be liable to be black listed/debarred for future works/ contract with BSNL. Any such action however be without prejudice to BSNL’s rights under the law.
3. In case supplier gets Blacklisted by GST authorities during the tenure of agreement with BSNL, supplier indemnifies BSNL from any monitory loss caused due such blacklisting i.e Loss of input credit claim etc and ensures that such loss will be paid to BSNL by the Bidder/supplier.

(Signature with Office Seal)
Date:
Location:

Witness:

(1) Signature-

Name……
S/o……
Address……
……

(2) Signature-

Name……
S/o……
Address……
……

Annexure VII

NO DEBAR/ BLACKLISTED DECLARATION

I /We…….. hereby declare that my/our firm has/have not been debarred for taking part in tender anywhere in any unit of BHARAT SANCHAR NIGA LIMITED. I/We also declared that my/ our firm is not under process of debarring by any unit of BSNL. I/We am/are aware that any suppression of facts in this regard/ breach of this condition/clause would result in immediate termination of contract/cancellation of the existing agreement and also forfeiting of my/our security deposit held.

Signature of Bidder/PWP

Name of Bidder/PWP

Capacity in which signing

Annexure VIII

DECLARATION (NO ADDITION /DELETION/ CORRECTION IN BID FORM)

I we …… hereby declare that “ No addition / deletion / corrections have been made in the downloaded EoI document being submitted and it is identical to the EoI document appearing on the website.”

Signature of PWP

Name of the PWP

(Capacity in which signing)

Annexure IX

CLAUSE BY CLAUSE COMPLIANCE

CLAUSE-BY-CLAUSE COMPLIANCE STATEMENT

Sl.	**CLAUSES**	**COMPLIANCE**
(A)	(B)	(C)
1.	All clauses of General Commercial Conditions of Part-I.	FULLY COMPLIED
2	All clauses of Financial Conditions of Part-II	FULLY COMPLIED
3	All clauses of Technical Conditions of Part-III	FULLY COMPLIED
4.	All clauses of Special Condition of **EoI** of PART-IV	FULLY COMPLIED
5.	All Annexures (Annexure-I to X)	FULLY COMPLIED

The clause-by-clause compliance statement should be given as per annexure..

The PWP should mention ‘FULLY COMPLIED’ in the column ‘C’ above, otherwise a statement of deviation may be submitted as per annexure.

Signature of PWP

Name of the PWP

(Capacity in which signing)

ANNEXURE-‘X’

NO DEVIATION STATEMENT

Sl.	CLAUSES	COMPLIANCE
(A)	(B)	(C)
1.	All clauses of General Commercial Conditions of Part-I.	No Deviation
2	All clauses of Financial Conditions of Part-II	No Deviation
3	All clauses of Technical Conditions of Part-III	No Deviation
4.	All clauses of Special Condition of EoI of PART-IV	No Deviation
5.	All Annexures (Annexure-I to XI)	No Deviation

The ‘No deviation statement’ should be given as per annexure.

The bidder should mention ‘ NO DEVIATION’ in the column ‘ C’ above, otherwise a statement of deviation may be submitted as per annexure.

Signature of PWP

Name of the PWP

(Capacity in which signing)