Request for Open Competitive Bid (OCB)

for

Selection of Service Provider for Supply, Installation of Network Firewall and Technical Support for Transport Department Offices across AP.

July 2022

Issued by

ANDHRA PRADESH TECHNOLOGY SERVICES LIMITED

(Government of AP Undertaking)

(CERT-In Empanelled and ISO 9001:2015, ISO 27001:2013 Certified)

3rd Floor, R&B Building, Opp. Indira Gandhi Municipal Stadium,

MG Road, Labbipet, Vijayawada-520010, Andhra Pradesh, India.

Ph.0866-2468102 | md_apts@ap.gov.in | https://www.apts.gov.in

Proprietary & Confidential

Contents

Section A – Schedule of Requirements

Tender Call Notice under Open Competitive Bidding Procedures for Selection of Service Provider for Supply, Installation of Network Firewall and Technical Support for Transport Department Offices across AP.

Time schedule of various tender related events:

Bid calling date	21-07-2022
Last date/time for Sale of document	03-08-2022, 02.30 PM
Bid closing date/time	03-08-2022, 03.00 PM
Bid opening date/time	03-08-2022, 03.30 PM
APTS Contact persons	Mr. K Raju, Manager (HWP4), Mob : 9963029405, email: raju.kollabathina@ap.gov.in
Bid Document Fee	Rs. 10,000/- To be paid through DD in the favour of The Managing Director, APTS Ltd, payable at Vijayawada or through online payment. **Bid document fee is exempted for bidders who participated in the previous calls for this tender.**
APTS Reference No.	APTS/HWP4/TRANSPORT-FIREWALL/2022/4

A.1. The solution, service or material required:

This tender call is issued on e-procurement marketplace at www.apeprocurement.gov.in. All the terms and conditions are to be read jointly as mentioned in the e-procurement market website and in this document.

APTS invites the bids from the interested parties for supply of Supply and Installation of Network Firewall and Technical Support for Transport Department Offices across AP., for a period of Five years from the date of signing of the contract agreement/LOI..

The detailed technical specifications of the items to be supplied are mentioned in Section -D.

A.2. Scope of incidental services:

Furnishing of a detailed operations and maintenance manual for each appropriate unit of the Supplied goods.

A.3. Maintenance:

Successful bidder has to supply, install & maintain all the items including re-installation of Operating system and other applications incase gets corrupted.

In case, the supplied items are down and not working, same need to be repaired and restored for normal functioning as per agreed Service Level Requirements. Failing which penalty will be recovered from Performance Security as per Clause C.

A.4. Delivery and Installation period:

Bidder shall deliver the goods/services, install and commission the same within **Eight (08)** weeks from the date of issue of Notification of Award / Date of issue of Purchase order, whichever is earlier. Hardware and Software are to be delivered and installed at Transport Commissioner head office and its 98 Branch locations.

A.5. Warranty:

Warranty period as specified in the BoM will start from the date of delivery or from the date of installation of items whichever is earlier.

During warranty period, bidder should attend for preventive maintenance of systems once in six months apart from regular service calls if any during the warranty period.

A.6. Order Placing Authority

1. APTS reserves the right not to place any supply / purchase order whatsoever, irrespective of finalization of the L1 bidder.
2. APTS/Department reserves the right to place purchase orders/ contracts as per RFP.
3. The RFP / contract does not confer any right whatsoever on the bidder/ successful Bidder in reverse auction for demanding APTS/any department to place order on them.

A.7.Preferential Market Access Policy:

G.O. Ms. No. 22, dt. 28-11-2015 issued by ITE&C Department & G.O. Ms. No. 9, Dt. 25-02-2021 issued by Industries & Commerce Department (copies can be obtained from URL: http://goir.ap.gov.in/Reports.aspx) are applicable for this tender. Bidders eligible for the benefits under preferential market access policy can apply by submitting all the relevant document proofs.

A.8 SLA for performance during warranty/maintenance period:

1. The original call log for all the logged calls of complaints & calls closed status should be sent by email to Department on monthly basis for monitoring.
2. Along with the above mentioned call log, a date wise abstract of calls logged and repair status within SLA and outside SLA shall be provided to APTS/Department in the following format with supporting call reports duly signed by the user:

		Calls closed						
Date	No.of calls logged	Within 24 hours	Within 48hrs	Within 72 hrs	Within 96hrs	Within 5 days	Within 10 days	Within 15days

3. The above table will be used for calculation of penalties for not meeting the SLA requirements during maintenance/warranty period. In case the information is not provided as mentioned above, a penalty of 0.2% of the total PO value for every week of delay or part thereof.

4. Persistent complaints from the user department during the warranty/maintenance period relating to the improper service will be sufficient ground for the APTS/Department to blacklist the successful bidder from participating in the future tenders.

A.9 Technical Demonstration

APTS may ask the bidders to demonstrate their offered devices before the Technical Committee for Technical Compliance.

A.10 Reverse Auction:

Process of Electronic Reverse Auction on eProcurement portal of Government of Andhra Pradesh

1. Reverse auction will be conducted on the total price for the contract period.
2. L1 bidder's prices are the tender inviting authorities' base prices for reverse auction.
3. Only the qualified bidders in financial stage will be permitted to participate in the reverse auction.
4. The date and time will be intimated to the qualified bidders.
5. For the purpose of Reverse Auction, the minimum bid decrement will be Rs. 10,000/-.
6. Bidders can modify the total schedule value based on the minimum bid decrement or the multiples thereof, to displace a standing lowest bid and become "L1", and this will continue as an iterative process.
7. The reverse auction shall be conducted for 3 Hours for each schedule, subsequently auto increment of 15 Minutes with every decrement that occurs within last 15 minutes. All bidders are required to submit their online bids during this period.
8. After the completion of the online reverse auction, the Closing Price (Final L1 Price) and the successful bidder shall be finalized. The closing price will be compared with prevailing market prices before issuing the NoA.
9. Within 1 Hour after conclusion of reverse auction, the successful bidder should upload the breakup of item wise cost components on eProcurement Portal.

Section B – Pre-qualification Criteria

1. The Bidder should be a manufacturer/ authorized representative of a manufacturer/wholesale dealer and should be in business of manufacture and or supply and maintenance of the IT & IT related equipment's for a minimum period of three (3) years in India as on bid calling date.
2. The Bidder should have at least one office with GST Registration in any of the 26 districts of AP. Billing/Invoice should be done from offices located in AP only. In case, Bidder does not have office in AP as on bid submission date, should submit an undertaking in Pre-qualification bid, to open the office in AP and register for AP GST. All Invoices should be raised with APGST Number only.
3. The Bidder should submit the Manufacturer's Authorization Form (MAF) for all the offered products / items, as per Annexure-III, specific to this tender issued by OEM authorizing the bidder to submit the bid for tendering which is deemed as an agreement in between the bidder and OEM for the support and spares till the warranty period.
4. The Bidder/OEM should have the following Service Centers / Franchise Service Centres in Prior to district re-organization districts in Andhra Pradesh as on bid submission date. The details are to be provided in Form P-4.

   Zone 1: Srikakulam/Vizianagaram/ Visakhapatnam
   Zone 2: East Godavari/West Godavari/ Krishna
   Zone 3: Guntur/Prakasam/Nellore
   Zone 4: Chittoor/Ananthapuram/Kadapa/ Kurnool

   Note: At least one Service Centers / Franchise Service Centres should have in each zone

   In case Bidder/OEM does not have the service centers/Franchise service center as on bid submission date, bidder/OEM should give an undertaking in PQ bid to open the service centers as specified above and should submit the Service Centers / Franchise service center details before the due date of Delivery in case the contract is awarded. Failing which the Purchaser may forfeit the PBG and cancel the contract.
5. The Bidder should have minimum average annual turnover of Rs. 6 Crore (IT & ITES Business) calculated over a period of the last three financial years i.e. 2018-19, 2019-20 & 2020-21. Certificate from CA to be submitted confirming the services.
6. Bidder should have positive net worth.
7. Bidder should have at least 3 years of experience in supplying, integrating and supporting network gateway security and routing technology solutions.

   a) Bidder must have provided heterogeneous (2 or more security and routing technologies in each deployment) Network Gateway security and routing solutions including firewall for at least 4 clients globally / India.

   b) Out of these, at least 2 orders should be of value greater than Rs. 1 Crore (either single or clubbed for the same customer) within last 3 years in India immediately preceding the date of this RFP.
8. The bidder should have significant client base in Government/Banking/Financial/Insurance sector in India under the relevant product/services.

9. The Bidder must be ISO 9001 Certified
10. The bidder should have back-to-back support with OEM of offered Firewall. Bidder should not be a mere reseller but a systems integrator. Bidder must have prime and direct (selling, support, upgrade and service) partnership with the solution / technology provider.
11. The bidder so selected should have the proven capability to perform the entire scope of the assignment without outsourcing the same to any third party.
12. The Bidder/OEM should furnish the information on major past supplies under the relevant product/services. The copies of the work orders for the last three financial years i.e. 2018-19, 2019-20 & 2020-21 should be submitted.
13. The bidder should submit/give declaration stating that they are not debarred/blacklisted by any State Government, Central Government, Central & State Govt. Undertakings/enterprises/Organizations and by any other Quasi Government bodies/Organizations in India for non-satisfactory performance, corrupt & Fraudulent or any other unethical business practices in Form P5.

    If the bidder is debarred/ blacklisted as mentioned above, such bidder becomes ineligible to participate in the bidding process. In case of any concealing of information relating to blacklisting or pending of cases as mentioned above or submission of fake information/fake documents, APTS reserves the right to cancel the work order/contract allotted, apart from forfeiting EMD/PBG. APTS reserves the right further to take penal action on the bidder.
14. Bidder from a country which shares a land border with India will be eligible to bid in this tender only if the bidder is registered with the Competent Authority as per G.O.Ms. No. 9, Dt. 25-02-2021 issued by Industries & Commerce Department, GoAP. DPIIT registration certificate copy to be submitted. Bidder shall have to submit the Undertaking as per FormP6.

Note: Relevant documents in support of above eligibility criteria should be furnished.

Section C – Statement of Important Limits/Values related to bid

<table>
<tr><th>S. No</th><th>Item</th><th>Description</th></tr>
<tr><td>1.</td><td>Earnest Money Deposit (EMD)</td><td>Rs.6,00,000/-. (Rupees Six Lakhs Only)

The EMD should be in the form of BG or through online payment only.

Scanned copy of EMD document should be uploaded on e-Procurement website. The Original EMD should be submitted to APTS before 5 pm of next working day after bid closing day.</td></tr>
<tr><td>2.</td><td>Bid Validity Period</td><td>90 days from the date of opening of bids.</td></tr>
<tr><td>3.</td><td>EMD Validity Period</td><td>Bank Guarantees that are issued by any Scheduled / Nationalized banks only will be accepted. BG Validity should be 135 days from the date of bid closing date.</td></tr>
<tr><td>4.</td><td>Contract Period</td><td>The contract period is 5 years from the date of signing of the agreement</td></tr>
<tr><td>5.</td><td>Evaluation of Bids</td><td>Bids will be evaluated tender wise</td></tr>
<tr><td>6.</td><td>Variation in Quantity</td><td>+/- 25%</td></tr>
<tr><td>7.</td><td>Period for furnishing performance security</td><td>Within 7 days from date of receipt of Notification of Award for the respective schedules.</td></tr>
<tr><td>8.</td><td>Performance security value with APTS/ Department</td><td>The bidder has to submit the PBG (3% of the Contract value/ Purchase Order Value) in favor of “The Managing Director, A.P. Technology Services Limited/ The Commissioner, Transport Department” from any Nationalized / Scheduled Bank before signing of the contract.</td></tr>
<tr><td>9.</td><td>Performance security validity period</td><td>60 days beyond Warranty period.</td></tr>
<tr><td>10.</td><td>Period for signing of contract</td><td>Within 7 days from date of receipt of Notification of Award.</td></tr>
<tr><td>11.</td><td>Payment terms</td><td>Payment authority: The Commissioner, Transport Department.

<table>
<tr><th>Payment terms</th><th>By Purchase order issuing authority</th></tr>
<tr><td>70% of contract / PO value</td><td>On delivery, successful installation and Acceptance Test for all locations.</td></tr>
<tr><td>Remaining 30% of the contract / PO value</td><td>In equal quarterly installment payment for 5 years.</td></tr>
<tr><td>Billing/Invoice</td><td>Billing/Invoice should be done from any of the offices located in AP only.</td></tr>
</table>
</td></tr>
</table>

12.	Terms for quarterly payment	On submission of the performance certificate by the respective Competent Authority as designated by the user department. The certificate/report should have Name, Designation, Signature, Phone number, Date and Seal of the Officer. **Effective date for start of Quarterly Payment:** Quarterly period starts after all the items are delivered, installed and certified by the department.
13.	Contracting Authority	The contract with the bidder will be entered by the Commissioner, Transport Department.
14.	LD for late deliveries/installation	**LD for late deliveries/Installations:** 1% of the late delivered or deemed late delivered/installed goods for One week or part thereof, 1.5% for Two weeks or part thereof, 2% for Three weeks or part thereof, 2.5% for 4 weeks or part thereof and so on.
15.	Maximum LD for late deliveries/ installation	Maximum LD for late deliveries/installations: 10% on the Total value of goods for that location/site for late delivery/installation or deemed late delivered/installed goods. However, APTS/Department reserves the right further to take penal action on the bidder. The bidder will be disqualified, blacklisted, action will be initiated as deemed fit and the Bid Security will be forfeited.
16.	Penalty for failure to maintain during warranty period for all items	Please refer to Section D: **IV) Service level Agreement (SLA)**
17.	Conditional bids	Not acceptable and liable for rejection
18.	Eligibility Criteria	As per Section B
19.	Transaction Fee & Corpus Fund	**Transaction fee:** All the participating bidders who submit the bids have to pay a) An amount@ 0.03% (plus GST) of their final bid value online with a cap of Rs. 10,000/- for quoted value of purchase up to Rs.50 Crore (or) b) An amount of Rs.25,000/- if the purchase value is above Rs.50crores plus GST applicable on transaction fee through online in favor of MD, APTS. The amount payable to APTS is nonrefundable. **Corpus Fund:** Successful bidder shall pay corpus fund in favor of MD, APTS through online (AP e-Procurement Portal) a) An amount @ 0.04% of the contract value with a cap of Rs.10,000/- (Rupees Ten Thousand Only) for contract value up to Rs.50 Crore (or)

		b) An amount of Rs.25,000/- (Rupees Twenty-Five Thousand Only) for the contract value above Rs.50 Crore.
20.	Bid submission	Online. a) Bidders are requested to submit the bids after issue of minutes of the pre bid meeting duly considering the changes made if any, during the pre-bid meeting. b) Bidders are totally responsible for incorporating/complying the changes/amendments issued if any during pre-bid meeting in their bid.
21.	Procedure for Bid Submission	Bids shall be submitted online on www.apeprocurement.gov.in platform 1. The participating bidders in the tender should register themselves free of cost on e-procurement platform in the website www.apeprocurement.gov.in. 2. Bidders can log-in to e-procurement platform in Secure mode only by signing with the Digital certificates. 3. The bidders who are desirous of participating in e-procurement shall submit their technical bids, price bids as per the standard formats available at the e-market place. 4. The bidders should scan and upload the respective documents in Pre-Qualification and Technical bid documentation as detailed at relevant sections of the RFP including EMD. The bidders shall sign on all the statements, documents certificates uploaded by them, owning responsibility for their correctness/authenticity. 5. The rates should be quoted in online only
22.	Other conditions	1. After uploading the documents, the copies of the uploaded statements, certificates, documents, original Demand Drafts in respect of Bid Security (except the Price bid/offer/break-up of taxes) are to be submitted by the bidder to the O/o The Managing Director, APTS, Vijayawada as and when required. 2. When asked, failure to furnish any of the uploaded documents, certificates, will entitle in rejection of the bid. 3. If any of the certificates, documents, etc., furnished by the Bidder are found to be false / fabricated / bogus, the bidder will be disqualified, blacklisted, action will be initiated as deemed fit and the Bid Security will be forfeited. 4. APTS will not hold any risk and responsibility regulating non-visibility of the scanned and uploaded documents. 5. The Documents that are uploaded online will only be considered for Bid Evaluation. 6. Important Notice to Contractors, Suppliers and Department users 7. In the endeavor to bring total automation of processes in e-Procurement, the Govt. has issued orders vide G.O.Ms.No.13, dated05.07.2006 permitting integration of electronic Payment Gateway of ICICI/HDFC/Axis Banks with e-Procurement

		platform, which provides a facility to participating suppliers / contractors to electronically pay the transaction fee online using their credit cards. 8. In case of consortium either the prime bidder or the consortium partner can purchase the bid document. The bid can be filed either with user ID of prime bidder or consortium partner.

Section D – Technical Specifications

I) Scope of work:

The key functional requirement of the project is shown below:

1. Ability to create granular security policy definitions per user and groups to identify, block or limit usage of web applications and widgets like instant messaging, social networking, video streaming, VoIP, games and more.
2. Provide application function control to identify, allow, block or limit usage of applications and features within them. Enable safe internet use while protecting against threats and malware.
3. Scan for viruses and malware in allowed collaborative applications.
4. Should have ability to protect environments with social media and internet applications.
5. TRANSPORT COMMISSIONER should have the power to create detailed policies that should be based on the characteristics such as user identity, user role and specific aspects of a web application.
6. There should be advanced user and application controls such as ability to expand user groups, domain names as well as detailed user and application usage information in reports, logs and statistics.
7. Should offer threat intelligence, mobile device security, Active Directory integration. Provide protection from zero day attacks and unknown threats.
8. Ability to integrate seamlessly with Active Directory to provide complete user identification and enable application based policy definition per user or group.
9. Virtual Private Network (VPN) technologies should be part of the solution to provide resilient and flexible site-to-site connectivity. Should have management tools to deploy, configure and operate the VPNs.
10. Identify and control applications sharing the same connection.
11. Should be able to intercept, decrypt and re-encrypt SSL/TLS, SSH, and VPN traffic with low performance degradation.
12. Decrypt outbound SSL.
13. Enable the same application visibility and control for remote users.
14. Deliver the same production throughput and performance with application control active.
15. Updates and upgrades to remote sites should be automated and performed seamlessly with the ability to view and manage remote operations through the central management system.
16. The product should have capability of deep packet inspection (DPI) to ensure various pieces of packet are thoroughly examined to identify malformed packets, errors, known attacks and other anomalies.

17. It should rapidly identify and block Trojans, viruses, spam, intrusion attempts and other violation of normal protocol communications.
18. Should have ability to manage security environment through intuitive graphical interface which should provide views, details and reports on security health through a comprehensive, centralized security dashboard.
19. The user interface and system configuration of the management console should be comprehensive, flexible and easy to use such that it should be possible to exclude features that are needed in the enterprise environment.
20. The network Firewall should be appliance based and rack mountable. Software based solutions are not acceptable.
21. The Successful bidder must analyze the existing production system and gather performance metrics. The successful bidder should review firewall system parameters such as sessions, resources, and drops to verify that the firewall is performing optimally. Additional checks should review traffic threat, and system logs to identify recommended changes as per best practices wherever applicable.
22. Establishing a procedure / SOPs for offline / online management of patches and upgrades.
23. Configuration & Testing of end-to-end connectivity using tunnel less IP Sec (Group Encrypted Transport VPN) at each location on new devices.
24. As TRANSPORT COMMISSIONER has dual bandwidth connectivity, successful Bidder shall terminate both the links to the new network firewall with automatic failover and ensure proper functionality as per existing setup at no extra cost to TRANSPORT COMMISSIONER.
25. The Successful Bidder shall be required to perform tasks, render requisite services and make available resources as may be required for the successful completion of the entire assignment at no additional cost to the TRANSPORT COMMISSIONER.
26. Bidder shall supply all necessary cables and power cords to make the network firewall functional.
27. In case of any change of location during the order & implementation, successful bidder must supply, install & configure accordingly without any extra cost to TRANSPORT COMMISSIONER.
28. **The L1 bidder should organize 1-day hands on training to the network team of transport department in each zone**

II) Items Detailed specifications as follows:

Item No.1: Firewalls – Qty: 67 Nos. (For UNIT/MVI/CP/TRACK Offices)

Sl.No.	Secure Network Termination Appliance Specifications
#	**Make & Model: <<Specify>>**
1	**General Requirements & Industry Certifications**
1.1	The proposed solution must provide Layer 7 / Application Layer security solution. The device proposed at the branch location must be able to natively identify and control applications, users and content
1.2	The proposed application security solution must be in the Leader's quadrant in the Gartner "Magic Quadrant for Enterprise Network Firewalls" from last 3 years.
1.3	For high performance with low latency the proposed solution must provide all application level inspection as real-time stream-based or using file-based store-and-forward techniques
1.4	The proposed solution must allow policy rule creation for application identification, user identification, host profile, threat prevention, content filtering, QOS and scheduling.
1.5	The Firewall appliance should have certifications like ICSA / EAL4 / NDPP or more
1.6	The Propose vendor must have track record continues improvement in threat detection and unique identification technologies.
1.7	The proposed appliance must have at least minimum 4 x 1G Ports
1.8	Firewall appliance should have console port and USB Ports
1.9	Appliance should be rack mountable and support side rails if required
1.10	Should support Internet Service Provider link load balancing.
2	**Performance**
2.1	The appliance must provide a minimum of **500 Mbps** Application enabled Firewall throughput and minimum **150 Mbps** of throughput with all security features enabled including Application Control + User Identification + IPS + Anti Spyware + Antivirus with all signatures on the appliance turned ON.
2.2	The proposed appliance must be able to handle minimum 30,000 new sessions per second
2.3	The proposed appliance must be able to handle minimum 2,00,000 concurrent sessions
2.4	The appliance must be capable of handling minimum 250 policies
2.5	The proposed appliance must be able to handle minimum 100 Mbps IPSEC VPN throughput
2.6	The proposed appliance must support minimum 200 Site to Site IPSEC VPN tunnels. The proposed solution must support minimum 250 client to site VPN tunnels. All licenses need to be provisioned from day one.
3	**Operation Mode**
3.1	The proposed appliance must support, Tap Mode, Transparent, Layer 2, Layer 3 mode providing flexible deployment. The proposed solution must be able to support simultaneous deployment with interfaces servicing Layer 3, Layer 2, Transparent and Tap modes.
3.2	The proposed appliance must support 802.1Q VLAN tagging
3.3	The proposed appliance must support Dual Stack IPv4 & IPv6 application control and threat inspection under various deployment modes from day one.
3.4	The proposed appliance must support standards based Link aggregation (IEEE 802.3ad) to achieve higher bandwidth
3.5	The proposed appliance must support logical Ethernet sub-interfaces tagged and untagged.
3.6	The proposed appliance must support the following routing protocols static, RIPv2, OSPF, BGP4

3.7	The proposed appliance must have Virtual Router capabilities that supports all L3 capabilities. The proposed solution must have IPv6 Static Routing Support even for virtual routers.
3.8	The proposed appliance must support DHCPv4 and DHCPv6 relay from day one.
3.9	**High Availability**
3.9.1	The proposed appliance must be able to support Active/passive configuration.
3.9.2	The proposed appliance must be able to support Active/Passive HA configuration
3.9.3	The proposed appliance must be capable to detect device, link and path failure and the ability to monitor health of the peer device without external network dependencies.
3.9.4	The proposed appliance must be able to support session and configuration synchronization
3.9.5	The proposed appliance must synchronize the following for HA . Sessions, Decryption Cert, Threat and Application Signature etc., ensuring seamless operations
3.9.6	The proposed appliance HA must support hitless upgrades for both major and minor code releases
3.10	The OEM must provide 24 X 7 X 365 technical support either directly or via authorized partners, with back-line support from the OEM. The OEM must have a local TAC in India
3.11	Every Gateway Security control (like Firewall or any other feature required to meet above specification) must not have any licensing restriction on number of users and must be supplied for unlimited users unless specified otherwise.
3.12	Should support at least 200 protocols (Optional).
3.13	All internet based applications should be supported for filtering like Telnet, FTP, SMTP, http, DNS, ICMP, DHCP, ARP, RPC, SNMP, Lotus Notes and Exchange etc.
3.14	Firewall should support the authentication protocols RADIUS, LDAP, TACACS, and PKI methods
3.15	Local access to the firewall modules should support authentication protocols – RADIUS & TACACS+.
3.16	Dynamic policy enforcement on VPN clients.
3.17	Firewall must provide state engine support for all common protocols of the TCP/IP stacks.
3.18	Should support telnet/SSH client and server functionality
4	**Firewall Security Policy**
4.1	The proposed solution must support network traffic classification which identifies applications across all ports irrespective of port/protocol/evasive tactic from day one. The proposed solution must have application and application function identification and decoding technology from day one.
4.2	The proposed solution must be able to handle unknown/unidentified applications e.g. alert, block or allow
4.3	The proposed solution must be able to create custom application signatures based on customer environment.
4.4	The proposed solution must delineate specific instances of peer2peer traffic (Bittorrent, emule, neonet, etc.), messaging (AIM, YIM, Facebook Chat, etc.) & Proxies (ultrasurf, ghostsurf, freegate, etc.).
4.5	The proposed solution must delineate different parts of the application such as allowing Facebook chat but blocking its file-transfer capability etc.
4.6	The proposed solution must support Voice based protocols (H.323, SIP, SCCP, MGCP etc.)
4.7	The proposed solution must support authentication services for user-identification using any of the following technologies AD, LDAP, eDirectory, Radius, Kerberos, Client Certificate from day one.
4.8	The proposed solution must support the creation of security policy based on Active Directory Users and Groups in addition to source/destination IP.

4.9	The proposed solution must support user-identification in policy without installing an agent on individual endpoints.
4.10	The proposed solution must populate and correlate all logs with user identity (traffic, IPS, URL, data, etc.) without any additional products or modules in real-time
4.11	The Firewall must provide NAT functionality, including dynamic and static NAT translations.
4.11.1	Network address translation (NAT) must be supported so that the private IP addresses of hosts and the structure of an internal network can be concealed by the firewall.
4.11.2	Network Address Translation (NAT) must be configurable as 1:1, 1: many, many: 1, many: many, flexible NAT (overlapping IPs). Reverse NAT must be supported.
4.11.3	Port address translation must be provided
4.12	The proposed solution must support Policy Based forwarding based on Zone, Applications , Source / Destination Address, User or User Group
5	**Threat Prevention Features**
5.1	The proposed solution shall support IPS , Anti Virus and Anti Bot & Spyware Protection features from day one.
5.2	The proposed solution shall be supported by a world-class threat research organization dedicated to the discovery and analysis of threats, applications and their respective network behavior. The threat and vulnerability information that is protected shall be publicly accessible on the internet.
5.3	The proposed solution shall block known network and application-layer vulnerability exploits
5.4	The proposed solution shall block buffer overflow, DoS/DDoS , etc., type of attacks
5.5	The proposed solution shall perform stream-based Anti-Virus & Anti-Spyware or store-and-forward traffic inspection
5.6	The proposed solution shall support attack recognition for IPv6 traffic the same way it does for IPv4
5.7	The proposed solution shall support Built-in Signature and Anomaly based Vulnerability Protection Engine
5.8	The proposed solution shall support the ability to create custom user-defined signatures
5.9	The proposed solution shall support granular tuning with option to configure overrides for individual signatures
5.10	The proposed solution shall support automatic security updates directly over a secure connection (i.e. no dependency of any intermediate device)
5.11	The proposed solution Vulnerability / Virus / Spyware protection signature updates shall not require reboot of the unit.
5.12	The proposed solution must support different actions in the policy such as deny, drop, reset client, reset server, reset both client and server.
5.13	Integrated IPS, Antivirus, Anti-Spyware & Anti-Bot functionality should be available as a module that can be activated and de-activated as and when required.
5.14	Activation of new IPS protections should be based on parameters like Threat severity i.e. High, Medium, low risk etc.
5.15	IPS Profile should have an option to select or re-select specific signatures that can be deactivated.
5.16	The proposed solution must have an option to add exceptions for network, services and Users.
5.17	The proposed solution must have functionality of Geo Protection to Block the traffic country wise.

5.18	The proposed solution must have an option to create your own signatures with an open signature language.
5.19	The proposed solution must provide detailed information on each protection, including: Vulnerability and threat descriptions, including CVE details & Threat severity
5.20	Solution must be able to identify malwares coming from incoming files and malwares downloaded from Internet
5.21	Solution must be able to Discover bot outbreaks
5.22	Solution must be able to discover the Bot infected machine
5.23	Solution must be able to prevent bot damage
5.24	Solution must have an Multi tier bot discovery i.e., Detect Command and Control IP/URL and DNS
5.25	Solution must be able to detect Unique communication patterns used by Botnets.
5.26	Solution must be able to block traffic between infected Host and Remote Operator and not to legitimate destination
5.27	Solution must be able to provide with Forensic tools which give details like Infected Users/Device, Malware type, Malware action etc.,
5.28	The proposed solution must support protection against credential phishing of internal users. The framework being used for protection has to be provided.
5.29	The Antivirus engine of the solution must be provided by the OEM itself and must not depend on a third party OEM for signatures
6	**SSL Decryption**
6.1	The proposed solution shall be able to identify, decrypt and evaluate SSL traffic in an outbound connection (forward-proxy)
6.2	The proposed solution shall be able to identify, decrypt and evaluate SSL traffic in an inbound connection
6.3	The proposed solution must support decryption and inspection of SSL traffic in an outbound connection, inbound connection across any port.
6.4	The proposed solution shall support the ability to have a SSL inspection policy differentiate between personal SSL connections i.e. banking, shopping, health and non-personal traffic.
6.5	The proposed solution must support on appliance Per policy SSL and SSH decryption for both inbound and outbound traffic.
6.6	The proposed must support on appliance SSL decryption policy based on IP, User, web category.
7	**URL Filtering**
7.1	The proposed solution shall support URL-Filtering, with the categorization being done by the OEM of the device and not a third party OEM.
7.2	The Proposed solution shall have the database located locally/ cache url category on the device
7.3	The proposed solution shall support custom URL-categorization
7.4	The proposed solution shall support customizable block pages
7.5	The proposed solution shall support logs populated with end user activity reports for site monitoring within the local solution
7.6	The proposed solution shall support Drive-by-download control
7.7	The proposed solution shall support URL Filtering policies by AD user, group, machines and IP address/range
7.8	The proposed solution must have the capability to provision additional authentication for specific URL categories for enhanced security.
8	**QOS**
8.1	The proposed firewall must support the ability to create QoS policy

8.1.1	by destination address
8.1.2	by user/user group as defined by AD
8.1.3	by application (such as Skype, Bit torrent, YouTube, azureus)
8.1.4	by static or dynamic application groups (such as Instant Messaging or P2P groups)
8.1.5	by port
8.2	The proposed firewall must define QoS traffic classes with:
8.2.1	guaranteed bandwidth
8.2.2	maximum bandwidth
8.2.3	priority queuing
8.3	The proposed firewall must support real-time prioritization of voice based protocols like H.323, SIP, SCCP, MGCP and applications like Skype.
8.4	The proposed firewall must support real-time bandwidth statistics of QoS classes.
9	**Management & Reporting**
9.1	The appliance shall provide local monitoring and reporting functionality, along with the ability to be managed and monitored from a remote management server from the same OEM. The management server shall be available in the virtual form factor.
9.2	The solution shall support the forwarding of logs to email/ external syslog servers and any other logging service / SIEM, as per customer requirements
9.3	The intelligence system of the OEM shall be publicly accessible (with applicable additionally procured licenses) to customers for threat analysis and proactive protection. This system shall provide historical data of all threats discovered by the OEM, it's indicators of compromise and applicable URLs, IP addresses, domains and hashes in searchable, taggable formats. This would allow Security administrators to search for specific indicators and use these indicators for improving security posture of the environment.
9.4	Firewall must support the user based logging. Log levels must be configurable based on severity.
9.5	It must be able to Search and Filter the log.
9.6	The Firewall logs must contain information about the firewall policy rule that triggered the log. Should support search of logs.
9.7	It must be able to correlate logs from various modules such as Firewall, Application Control, Antivirus & information at different periods of Time.
9.8	It must support SNMP (Simple Network Management Protocol) v 2.0 and v 3.0.
9.9	The firewall must be capable of integrating with other equipment like SIEM tool or reporting tools etc.
9.10	The solution must be commonly integrated with any of the SIEM products, with no customization needed for integration.
9.11	The proposed solution shall populate and correlate all logs with user identity (traffic, IPS, URL, data, AV, AB etc.) without any additional products or modules in real-time
9.12	Application and user identify based bandwidth management
9.13	Guaranteed &Burstable bandwidth policy
9.14	Bandwidth monitoring
9.15	The management system must support the ability to lock configuration while modifying it, avoiding administrator collision when there are multiple people configuring the appliance

Item No.2: Firewalls – Qty: 31 Nos. (For DTO/RTO Offices)

Sl.No.	Secure Network Termination Appliance Specifications
#	**Make & Model: <<Specify>>**

1	**General Requirements & Industry Certifications**
1.1	The proposed solution must provide Layer 7 / Application Layer security solution. The device proposed at the branch location must be able to natively identify and control applications, users and content
1.2	The proposed application security solution must be in the Leader's quadrant in the Gartner "Magic Quadrant for Enterprise Network Firewalls" from last 3 years.
1.3	For high performance with low latency the proposed solution must provide all application level inspection as real-time stream-based or using file-based store-and-forward techniques
1.4	The proposed solution must allow policy rule creation for application identification, user identification, host profile, threat prevention, content filtering, QOS and scheduling.
1.5	The Firewall appliance should have certifications like ICSA / EAL4 / NDPP or more
1.6	The Propose vendor must have track record continues improvement in threat detection and unique identification technologies.
1.7	The proposed appliance must have at least minimum 6 x 1G Ports
1.8	Firewall appliance should have console port and USB Ports
1.9	Appliance should be rack mountable and support side rails if required
1.10	Should support Internet Service Provider link load balancing.
2	**Performance**
2.1	The appliance must provide a minimum of **1 Gbps** Application enabled Firewall throughput and minimum **300 Mbps** of throughput with all security features enabled including Application Control + User Identification + IPS + Anti Spyware + Antivirus with all signatures on the appliance turned ON.
2.2	The proposed appliance must be able to handle minimum 30,000 new sessions per second
2.3	The proposed appliance must be able to handle minimum 2,00,000 concurrent sessions
2.4	The appliance must be capable of handling minimum 250 policies
2.5	The proposed appliance must be able to handle minimum 100 Mbps IPSEC VPN throughput
2.6	The proposed appliance must support minimum 200 Site to Site IPSEC VPN tunnels. The proposed solution must support minimum 250 client to site VPN tunnels. All licenses need to be provisioned from day one.
3	**Operation Mode**
3.1	The proposed appliance must support, Tap Mode, Transparent, Layer 2, Layer 3 mode providing flexible deployment. The proposed solution must be able to support simultaneous deployment with interfaces servicing Layer 3, Layer 2, Transparent and Tap modes.
3.2	The proposed appliance must support 802.1Q VLAN tagging
3.3	The proposed appliance must support Dual Stack IPv4 & IPv6 application control and threat inspection under various deployment modes from day one.
3.4	The proposed appliance must support standards based Link aggregation (IEEE 802.3ad) to achieve higher bandwidth
3.5	The proposed appliance must support logical Ethernet sub-interfaces tagged and untagged.
3.6	The proposed appliance must support the following routing protocols static, RIPv2, OSPF, BGP4
3.7	The proposed appliance must have Virtual Router capabilities that supports all L3 capabilities. The proposed solution must have IPv6 Static Routing Support even for virtual routers.
3.8	The proposed appliance must support DHCPv4 and DHCPv6 relay from day one.
3.9	**High Availability**
3.9.1	The proposed appliance must be able to support Active/passive configuration.
3.9.2	The proposed appliance must be able to support Active/Passive HA configuration

3.9.3	The proposed appliance must be capable to detect device, link and path failure and the ability to monitor health of the peer device without external network dependencies.
3.9.4	The proposed appliance must be able to support session and configuration synchronization
3.9.5	The proposed appliance must synchronize the following for HA . Sessions, Decryption Cert, Threat and Application Signature etc., ensuring seamless operations
3.9.6	The proposed appliance HA must support hitless upgrades for both major and minor code releases
3.10	The OEM must provide 24 X 7 X 365 technical support either directly or via authorized partners, with back-line support from the OEM. The OEM must have a local TAC in India
3.11	Every Gateway Security control (like Firewall or any other feature required to meet above specification) must not have any licensing restriction on number of users and must be supplied for unlimited users unless specified otherwise.
3.12	Should support at least 200 protocols (Optional).
3.13	All internet based applications should be supported for filtering like Telnet, FTP, SMTP, http, DNS, ICMP, DHCP, ARP, RPC, SNMP, Lotus Notes and Exchange etc.
3.14	Firewall should support the authentication protocols RADIUS, LDAP, TACACS, and PKI methods
3.15	Local access to the firewall modules should support authentication protocols – RADIUS & TACACS+.
3.16	Dynamic policy enforcement on VPN clients.
3.17	Firewall must provide state engine support for all common protocols of the TCP/IP stacks.
3.18	Should support telnet/SSH client and server functionality
4	**Firewall Security Policy**
4.1	The proposed solution must support network traffic classification which identifies applications across all ports irrespective of port/protocol/evasive tactic from day one. The proposed solution must have application and application function identification and decoding technology from day one.
4.2	The proposed solution must be able to handle unknown/unidentified applications e.g. alert, block or allow
4.3	The proposed solution must be able to create custom application signatures based on customer environment.
4.4	The proposed solution must delineate specific instances of peer2peer traffic (Bittorrent, emule, neonet, etc.), messaging (AIM, YIM, Facebook Chat, etc.) & Proxies (ultrasurf, ghostsurf, freegate, etc.).
4.5	The proposed solution must delineate different parts of the application such as allowing Facebook chat but blocking its file-transfer capability etc.
4.6	The proposed solution must support Voice based protocols (H.323, SIP, SCCP, MGCP etc.)
4.7	The proposed solution must support authentication services for user-identification using any of the following technologies AD, LDAP, eDirectory, Radius, Kerberos, Client Certificate from day one.
4.8	The proposed solution must support the creation of security policy based on Active Directory Users and Groups in addition to source/destination IP.
4.9	The proposed solution must support user-identification in policy without installing an agent on individual endpoints.
4.10	The proposed solution must populate and correlate all logs with user identity (traffic, IPS, URL, data, etc.) without any additional products or modules in real-time
4.11	The Firewall must provide NAT functionality, including dynamic and static NAT translations.

4.11.1	Network address translation (NAT) must be supported so that the private IP addresses of hosts and the structure of an internal network can be concealed by the firewall.
4.11.2	Network Address Translation (NAT) must be configurable as 1:1, 1: many, many: 1, many: many, flexible NAT (overlapping IPs). Reverse NAT must be supported.
4.11.3	Port address translation must be provided
4.12	The proposed solution must support Policy Based forwarding based on Zone, Applications , Source / Destination Address, User or User Group
5	**Threat Prevention Features**
5.1	The proposed solution shall support IPS , Anti Virus and Anti Bot & Spyware Protection features from day one.
5.2	The proposed solution shall be supported by a world-class threat research organization dedicated to the discovery and analysis of threats, applications and their respective network behavior. The threat and vulnerability information that is protected shall be publicly accessible on the internet.
5.3	The proposed solution shall block known network and application-layer vulnerability exploits
5.4	The proposed solution shall block buffer overflow, DoS/DDoS , etc., type of attacks
5.5	The proposed solution shall perform stream-based Anti-Virus & Anti-Spyware or store-and-forward traffic inspection
5.6	The proposed solution shall support attack recognition for IPv6 traffic the same way it does for IPv4
5.7	The proposed solution shall support Built-in Signature and Anomaly based Vulnerability Protection Engine
5.8	The proposed solution shall support the ability to create custom user-defined signatures
5.9	The proposed solution shall support granular tuning with option to configure overrides for individual signatures
5.10	The proposed solution shall support automatic security updates directly over a secure connection (i.e. no dependency of any intermediate device)
5.11	The proposed solution Vulnerability / Virus / Spyware protection signature updates shall not require reboot of the unit.
5.12	The proposed solution must support different actions in the policy such as deny, drop, reset client, reset server, reset both client and server.
5.13	Integrated IPS, Antivirus, Anti-Spyware & Anti-Bot functionality should be available as a module that can be activated and de-activated as and when required.
5.14	Activation of new IPS protections should be based on parameters like Threat severity i.e. High, Medium, low risk etc.
5.15	IPS Profile should have an option to select or re-select specific signatures that can be deactivated.
5.16	The proposed solution must have an option to add exceptions for network, services and Users.
5.17	The proposed solution must have functionality of Geo Protection to Block the traffic country wise.
5.18	The proposed solution must have an option to create your own signatures with an open signature language.
5.19	The proposed solution must provide detailed information on each protection, including: Vulnerability and threat descriptions, including CVE details & Threat severity
5.20	Solution must be able to identify malwares coming from incoming files and malwares downloaded from Internet
5.21	Solution must be able to Discover bot outbreaks

5.22	Solution must be able to discover the Bot infected machine
5.23	Solution must be able to prevent bot damage
5.24	Solution must have an Multi tier bot discovery i.e., Detect Command and Control IP/URL and DNS
5.25	Solution must be able to detect Unique communication patterns used by Botnets.
5.26	Solution must be able to block traffic between infected Host and Remote Operator and not to legitimate destination
5.27	Solution must be able to provide with Forensic tools which give details like Infected Users/Device, Malware type, Malware action etc.,
5.28	The proposed solution must support protection against credential phishing of internal users. The framework being used for protection has to be provided.
5.29	The Antivirus engine of the solution must be provided by the OEM itself and must not depend on a third party OEM for signatures
6	**SSL Decryption**
6.1	The proposed solution shall be able to identify, decrypt and evaluate SSL traffic in an outbound connection (forward-proxy)
6.2	The proposed solution shall be able to identify, decrypt and evaluate SSL traffic in an inbound connection
6.3	The proposed solution must support decryption and inspection of SSL traffic in an outbound connection, inbound connection across any port.
6.4	The proposed solution shall support the ability to have a SSL inspection policy differentiate between personal SSL connections i.e. banking, shopping, health and non-personal traffic.
6.5	The proposed solution must support on appliance Per policy SSL and SSH decryption for both inbound and outbound traffic.
6.6	The proposed must support on appliance SSL decryption policy based on IP, User, web category.
7	**URL Filtering**
7.1	The proposed solution shall support URL-Filtering, with the categorization being done by the OEM of the device and not a third party OEM.
7.2	The Proposed solution shall have the database located locally/ cache url category on the device
7.3	The proposed solution shall support custom URL-categorization
7.4	The proposed solution shall support customizable block pages
7.5	The proposed solution shall support logs populated with end user activity reports for site monitoring within the local solution
7.6	The proposed solution shall support Drive-by-download control
7.7	The proposed solution shall support URL Filtering policies by AD user, group, machines and IP address/range
7.8	The proposed solution must have the capability to provision additional authentication for specific URL categories for enhanced security.
8	**QOS**
8.1	The proposed firewall must support the ability to create QoS policy
8.1.1	by destination address
8.1.2	by user/user group as defined by AD
8.1.3	by application (such as Skype, Bit torrent, YouTube, azureus)
8.1.4	by static or dynamic application groups (such as Instant Messaging or P2P groups)
8.1.5	by port
8.2	The proposed firewall must define QoS traffic classes with:
8.2.1	guaranteed bandwidth

8.2.2	maximum bandwidth
8.2.3	priority queuing
8.3	The proposed firewall must support real-time prioritization of voice based protocols like H.323, SIP, SCCP, MGCP and applications like Skype.
8.4	The proposed firewall must support real-time bandwidth statistics of QoS classes.
9	**Management & Reporting**
9.1	The appliance shall provide local monitoring and reporting functionality, along with the ability to be managed and monitored from a remote management server from the same OEM. The management server shall be available in the virtual form factor.
9.2	The solution shall support the forwarding of logs to email/ external syslog servers and any other logging service / SIEM, as per customer requirements
9.3	The intelligence system of the OEM shall be publicly accessible (with applicable additionally procured licenses) to customers for threat analysis and proactive protection. This system shall provide historical data of all threats discovered by the OEM, it's indicators of compromise and applicable URLs, IP addresses, domains and hashes in searchable, taggable formats. This would allow Security administrators to search for specific indicators and use these indicators for improving security posture of the environment.
9.4	Firewall must support the user based logging. Log levels must be configurable based on severity.
9.5	It must be able to Search and Filter the log.
9.6	The Firewall logs must contain information about the firewall policy rule that triggered the log. Should support search of logs.
9.7	It must be able to correlate logs from various modules such as Firewall, Application Control, Antivirus & information at different periods of Time.
9.8	It must support SNMP (Simple Network Management Protocol) v 2.0 and v 3.0.
9.9	The firewall must be capable of integrating with other equipment like SIEM tool or reporting tools etc.
9.10	The solution must be commonly integrated with any of the SIEM products, with no customization needed for integration.
9.11	The proposed solution shall populate and correlate all logs with user identity (traffic, IPS, URL, data, AV, AB etc.) without any additional products or modules in real-time
9.12	Application and user identify based bandwidth management
9.13	Guaranteed &Burstable bandwidth policy
9.14	Bandwidth monitoring
9.15	The management system must support the ability to lock configuration while modifying it, avoiding administrator collision when there are multiple people configuring the appliance

Item No.3: Firewall – Qty: 1 No. (For Head Office)

Sl.No.	Secure Network Termination Appliance Specifications
#	**Make & Model: <<Specify>>**
1	**General Requirements & Industry Certifications**
1.1	The proposed solution must provide Layer 7 / Application Layer security solution. The device proposed at the branch location must be able to natively identify and control applications, users and content
1.2	The proposed application security solution must be in the Leader's quadrant in the Gartner "Magic Quadrant for Enterprise Network Firewalls" from last 3 years.
1.3	For high performance with low latency the proposed solution must provide all application level inspection as real-time stream-based or using file-based store-and-forward techniques

1.4	The proposed solution must allow policy rule creation for application identification, user identification, host profile, threat prevention, content filtering, QOS and scheduling.
1.5	The Firewall appliance should have certifications like ICSA / EAL4 / NDPP or more
1.6	The Propose vendor must have track record continues improvement in threat detection and unique identification technologies.
1.7	The proposed appliance must have at least minimum 8 x 1G Ports atleast 2 Fiber Ports
1.8	Firewall appliance should have console port and USB Ports
1.9	Appliance should be rack mountable and support side rails if required
1.10	Should support Internet Service Provider link load balancing.
2	**Performance**
2.1	The appliance must provide a minimum of **2 Gbps** Application enabled Firewall throughput and minimum **1 Gbps** of throughput with all security features enabled including Application Control + User Identification + IPS + Anti Spyware + Antivirus with all signatures on the appliance turned ON.
2.2	The proposed appliance must be able to handle minimum 30,000 new sessions per second
2.3	The proposed appliance must be able to handle minimum 2,00,000 concurrent sessions
2.4	The appliance must be capable of handling minimum 250 policies
2.5	The proposed appliance must be able to handle minimum 100 Mbps IPSEC VPN throughput
2.6	The proposed appliance must support minimum 250 Site to Site IPSEC VPN tunnels. The proposed solution must support minimum 250 client to site VPN tunnels. All licenses need to be provisioned from day one.
3	**Operation Mode**
3.1	The proposed appliance must support, Tap Mode, Transparent, Layer 2, Layer 3 mode providing flexible deployment. The proposed solution must be able to support simultaneous deployment with interfaces servicing Layer 3, Layer 2, Transparent and Tap modes.
3.2	The proposed appliance must support 802.1Q VLAN tagging
3.3	The proposed appliance must support Dual Stack IPv4 & IPv6 application control and threat inspection under various deployment modes from day one.
3.4	The proposed appliance must support standards based Link aggregation (IEEE 802.3ad) to achieve higher bandwidth
3.5	The proposed appliance must support logical Ethernet sub-interfaces tagged and untagged.
3.6	The proposed appliance must support the following routing protocols static, RIPv2, OSPF, BGP4
3.7	The proposed appliance must have Virtual Router capabilities that supports all L3 capabilities. The proposed solution must have IPv6 Static Routing Support even for virtual routers.
3.8	The proposed appliance must support DHCPv4 and DHCPv6 relay from day one.
3.9	**High Availability**
3.9.1	The proposed appliance must be able to support Active/passive configuration.
3.9.2	The proposed appliance must be able to support Active/Passive HA configuration
3.9.3	The proposed appliance must be capable to detect device, link and path failure and the ability to monitor health of the peer device without external network dependencies.
3.9.4	The proposed appliance must be able to support session and configuration synchronization
3.9.5	The proposed appliance must synchronize the following for HA . Sessions, Decryption Cert, Threat and Application Signature etc., ensuring seamless operations
3.9.6	The proposed appliance HA must support hitless upgrades for both major and minor code releases
3.10	The OEM must provide 24 X 7 X 365 technical support either directly or via authorized partners, with back-line support from the OEM. The OEM must have a local TAC in India

3.11	Every Gateway Security control (like Firewall or any other feature required to meet above specification) must not have any licensing restriction on number of users and must be supplied for unlimited users unless specified otherwise.
3.12	Should support at least 200 protocols (Optional).
3.13	All internet based applications should be supported for filtering like Telnet, FTP, SMTP, http, DNS, ICMP, DHCP, ARP, RPC, SNMP, Lotus Notes and Exchange etc.
3.14	Firewall should support the authentication protocols RADIUS, LDAP, TACACS, and PKI methods
3.15	Local access to the firewall modules should support authentication protocols – RADIUS & TACACS+.
3.16	Dynamic policy enforcement on VPN clients.
3.17	Firewall must provide state engine support for all common protocols of the TCP/IP stacks.
3.18	Should support telnet/SSH client and server functionality
4	**Firewall Security Policy**
4.1	The proposed solution must support network traffic classification which identifies applications across all ports irrespective of port/protocol/evasive tactic from day one. The proposed solution must have application and application function identification and decoding technology from day one.
4.2	The proposed solution must be able to handle unknown/unidentified applications e.g. alert, block or allow
4.3	The proposed solution must be able to create custom application signatures based on customer environment.
4.4	The proposed solution must delineate specific instances of peer2peer traffic (Bittorrent, emule, neonet, etc.), messaging (AIM, YIM, Facebook Chat, etc.) & Proxies (ultrasurf, ghostsurf, freegate, etc.).
4.5	The proposed solution must delineate different parts of the application such as allowing Facebook chat but blocking its file-transfer capability etc.
4.6	The proposed solution must support Voice based protocols (H.323, SIP, SCCP, MGCP etc.)
4.7	The proposed solution must support authentication services for user-identification using any of the following technologies AD, LDAP, eDirectory, Radius, Kerberos, Client Certificate from day one.
4.8	The proposed solution must support the creation of security policy based on Active Directory Users and Groups in addition to source/destination IP.
4.9	The proposed solution must support user-identification in policy without installing an agent on individual endpoints.
4.10	The proposed solution must populate and correlate all logs with user identity (traffic, IPS, URL, data, etc.) without any additional products or modules in real-time
4.11	The Firewall must provide NAT functionality, including dynamic and static NAT translations.
4.11.1	Network address translation (NAT) must be supported so that the private IP addresses of hosts and the structure of an internal network can be concealed by the firewall.
4.11.2	Network Address Translation (NAT) must be configurable as 1:1, 1: many, many: 1, many: many, flexible NAT (overlapping IPs). Reverse NAT must be supported.
4.11.3	Port address translation must be provided
4.12	The proposed solution must support Policy Based forwarding based on Zone, Applications , Source / Destination Address, User or User Group
5	**Threat Prevention Features**
5.1	The proposed solution shall support IPS , Anti Virus and Anti Bot & Spyware Protection features from day one.

5.2	The proposed solution shall be supported by a world-class threat research organization dedicated to the discovery and analysis of threats, applications and their respective network behavior. The threat and vulnerability information that is protected shall be publicly accessible on the internet.
5.3	The proposed solution shall block known network and application-layer vulnerability exploits
5.4	The proposed solution shall block buffer overflow, DoS/DDoS , etc., type of attacks
5.5	The proposed solution shall perform stream-based Anti-Virus & Anti-Spyware or store-and-forward traffic inspection
5.6	The proposed solution shall support attack recognition for IPv6 traffic the same way it does for IPv4
5.7	The proposed solution shall support Built-in Signature and Anomaly based Vulnerability Protection Engine
5.8	The proposed solution shall support the ability to create custom user-defined signatures
5.9	The proposed solution shall support granular tuning with option to configure overrides for individual signatures
5.10	The proposed solution shall support automatic security updates directly over a secure connection (i.e. no dependency of any intermediate device)
5.11	The proposed solution Vulnerability / Virus / Spyware protection signature updates shall not require reboot of the unit.
5.12	The proposed solution must support different actions in the policy such as deny, drop, reset client, reset server, reset both client and server.
5.13	Integrated IPS, Antivirus, Anti-Spyware & Anti-Bot functionality should be available as a module that can be activated and de-activated as and when required.
5.14	Activation of new IPS protections should be based on parameters like Threat severity i.e. High, Medium, low risk etc.
5.15	IPS Profile should have an option to select or re-select specific signatures that can be deactivated.
5.16	The proposed solution must have an option to add exceptions for network, services and Users.
5.17	The proposed solution must have functionality of Geo Protection to Block the traffic country wise.
5.18	The proposed solution must have an option to create your own signatures with an open signature language.
5.19	The proposed solution must provide detailed information on each protection, including: Vulnerability and threat descriptions, including CVE details & Threat severity
5.20	Solution must be able to identify malwares coming from incoming files and malwares downloaded from Internet
5.21	Solution must be able to Discover bot outbreaks
5.22	Solution must be able to discover the Bot infected machine
5.23	Solution must be able to prevent bot damage
5.24	Solution must have an Multi tier bot discovery i.e., Detect Command and Control IP/URL and DNS
5.25	Solution must be able to detect Unique communication patterns used by Botnets.
5.26	Solution must be able to block traffic between infected Host and Remote Operator and not to legitimate destination
5.27	Solution must be able to provide with Forensic tools which give details like Infected Users/Device, Malware type, Malware action etc.,

5.28	The proposed solution must support protection against credential phishing of internal users. The framework being used for protection has to be provided.
5.29	The Antivirus engine of the solution must be provided by the OEM itself and must not depend on a third party OEM for signatures
6	**SSL Decryption**
6.1	The proposed solution shall be able to identify, decrypt and evaluate SSL traffic in an outbound connection (forward-proxy)
6.2	The proposed solution shall be able to identify, decrypt and evaluate SSL traffic in an inbound connection
6.3	The proposed solution must support decryption and inspection of SSL traffic in an outbound connection, inbound connection across any port.
6.4	The proposed solution shall support the ability to have a SSL inspection policy differentiate between personal SSL connections i.e. banking, shopping, health and non-personal traffic.
6.5	The proposed solution must support on appliance Per policy SSL and SSH decryption for both inbound and outbound traffic.
6.6	The proposed must support on appliance SSL decryption policy based on IP, User, web category.
7	**URL Filtering**
7.1	The proposed solution shall support URL-Filtering, with the categorization being done by the OEM of the device and not a third party OEM.
7.2	The Proposed solution shall have the database located locally/ cache url category on the device
7.3	The proposed solution shall support custom URL-categorization
7.4	The proposed solution shall support customizable block pages
7.5	The proposed solution shall support logs populated with end user activity reports for site monitoring within the local solution
7.6	The proposed solution shall support Drive-by-download control
7.7	The proposed solution shall support URL Filtering policies by AD user, group, machines and IP address/range
7.8	The proposed solution must have the capability to provision additional authentication for specific URL categories for enhanced security.
8	**QOS**
8.1	The proposed firewall must support the ability to create QoS policy
8.1.1	by destination address
8.1.2	by user/user group as defined by AD
8.1.3	by application (such as Skype, Bit torrent, YouTube, azureus)
8.1.4	by static or dynamic application groups (such as Instant Messaging or P2P groups)
8.1.5	by port
8.2	The proposed firewall must define QoS traffic classes with:
8.2.1	guaranteed bandwidth
8.2.2	maximum bandwidth
8.2.3	priority queuing
8.3	The proposed firewall must support real-time prioritization of voice based protocols like H.323, SIP, SCCP, MGCP and applications like Skype.
8.4	The proposed firewall must support real-time bandwidth statistics of QoS classes.
9	**Management & Reporting**
9.1	The appliance shall provide local monitoring and reporting functionality, along with the ability to be managed and monitored from a remote management server from the same OEM. The management server shall be available in the virtual form factor.

9.2	The solution shall support the forwarding of logs to email/ external syslog servers and any other logging service / SIEM, as per customer requirements
9.3	The intelligence system of the OEM shall be publicly accessible (with applicable additionally procured licenses) to customers for threat analysis and proactive protection. This system shall provide historical data of all threats discovered by the OEM, it's indicators of compromise and applicable URLs, IP addresses, domains and hashes in searchable, taggable formats. This would allow Security administrators to search for specific indicators and use these indicators for improving security posture of the environment.
9.4	Firewall must support the user based logging. Log levels must be configurable based on severity.
9.5	It must be able to Search and Filter the log.
9.6	The Firewall logs must contain information about the firewall policy rule that triggered the log. Should support search of logs.
9.7	It must be able to correlate logs from various modules such as Firewall, Application Control, Antivirus & information at different periods of Time.
9.8	It must support SNMP (Simple Network Management Protocol) v 2.0 and v 3.0.
9.9	The firewall must be capable of integrating with other equipment like SIEM tool or reporting tools etc.
9.10	The solution must be commonly integrated with any of the SIEM products, with no customization needed for integration.
9.11	The proposed solution shall populate and correlate all logs with user identity (traffic, IPS, URL, data, AV, AB etc.) without any additional products or modules in real-time
9.12	Application and user identify based bandwidth management
9.13	Guaranteed &Burstable bandwidth policy
9.14	Bandwidth monitoring
9.15	The management system must support the ability to lock configuration while modifying it, avoiding administrator collision when there are multiple people configuring the appliance

III) Service Level Expectations (SLEs)

a. During the warranty period the following service levels are expected to be maintained by the Vendor / Successful Bidder.

b. Breach of service levels consistently on part of the Vendor / Successful Bidder may lead to invocation of Clause for "Termination for Default"

c. 99.9% uptime is expected for all devices and would be calculated on quarterly basis.

d. Any problem / issues / defects in Firewall appliances, enhancement requests reported to the Vendor / Successful Bidder should be categorized based on severity as follows:

i. Issue resolution / Onsite visits within 24 hrs for Head of the department and 26 District Head Quarters issues.
ii. Issues resolution / Onsite visits within 48 hrs for remaining Head of the department and 26 District Head Quarters issues.
iii. Return Material Authorization (RMA) support
iv. Annual Firewall Rule Base review (Audit)

e. System Maintenance & Support services will include the following activities.

- 24 x 7 online support

- Onsite patch updation and major / minor software version
- Onsite training to be provided to key users.

f. For RMA (Return Material Authorization) the turnaround expected is as below.

RMA Support should be valid for 24 x 7 with a response time of 24 hours and replacement within 1 business day.

IV) Service level Agreement (SLA)

The vendor has to ensure adherence to time schedules given in this RFP. Non-adherence will attract penalties as given below.

Sl. No.	Description of Delay	Penalty
1.	Delivery of all software & hardware security products needed as per the expected deliverables within permitted delivery period from the date of receipt of the purchase order.	1% of the late delivered or deemed late delivered/installed goods for One week or part thereof, 1.5% for Two weeks or part thereof, 2% for Three weeks or part thereof, 2.5% for 4 weeks or part thereof and so on.
2.	Delay in implementation of all devices beyond 6 weeks from the date of receipt of the purchase order.	1% of the late delivered or deemed late delivered/installed goods for One week or part thereof, 1.5% for Two weeks or part thereof, 2% for Three weeks or part thereof, 2.5% for 4 weeks or part thereof and so on.
3.	Delay in submission documentation	0.2% of the total PO value for every week of delay or part thereof.
4.	In case of a breakdown of appliances/ malfunctioning of hardware, hardware components accessories, systems software, and/or any products, the relevant defect should be attended immediately and rectified within 1 days of the receipt/notice of the complaint.	0.2% of the item value per each hour of delay or part thereof.
5.	In case both the appliances/hardware in the HA mode are down and the system is completely down the defect should be attended and rectified within 4 hours of receipt of notice.	0.2% of the item value per every 1 hour of delay or part thereof.
6.	Failure to prevent attacks for which the solutions has been procured.	20% of the Quarterly amount.
7.	Delay in posting of offsite support Personnel beyond 4 weeks from the date of issue of purchase order for security products.	0.5% of the purchase order value per week of delay or part thereof.
8.	Delay in providing details for offsite support beyond 4 weeks from date of issue of PO	Rs.1,000/- per day.

9.	Delay in providing complete escalation matrix for offsite support beyond 4 weeks from date of issue of PO	Rs.1,000/- per day.
10.	Delay in installation of patches, updates and upgrades	If the patches/signature files are not deployed within a period of 5 working days of TRANSPORT COMMISSIONER from the release of latest version/update by OEM, it will attract a penalty of 0.5% of the charges from quarterly amount on-site & remote monitoring services for each week of delay or part thereof.
11.	If the TRANSPORT COMMISSIONER firewall system uptime for any of the locations is below 99.9% calculated on quarterly basis.	2% of onsite and offsite support charges of every 0.1% decrease of system uptime for that location.
12.	Head of the department and 26 District Head Quarters issues specified in Section D clause III (SLEs)	Beyond 24hrs Rs.5,000/- for each day till the Resolution of the issue.
13.	Remaining Head of the department and 26 District Head Quarters issues specified in Section D clause III (SLEs)	Beyond 48hrs Rs.5,000/- for each day till the resolution of the issue
14.	Return Material Authorization (RMA) Support in Section D clause III (SLEs)	Response and Replacement Beyond 24 hours penalty of Rs. 10,000/- per day
15.	Annual Firewall Base Review	Should be done Every year in the month of January. Beyond this month, Rs.10,000/- per week.

Exclusions from downtime calculation include the following

1. Downtime because of LAN cabling faults.
2. Scheduled downtimes (which are approved by TRANSPORT COMMISSIONER) on account of preventive maintenance, system testing, system upgrades etc.
3. All failures due to source power unavailability and power conditioning, UPS failure etc. beyond control of Vendor Managed Services.
4. Force Majeure conditions defined above or any condition not foreseen but mutually agreed by both the parties.
5. Link outages owing to ISPs.
6. Downtime due to any device/appliance not managed by the Vendor.

V) User Acceptance Test (UAT)

a. TRANSPORT COMMISSIONER reserves the right to carry out inspection and / or test any components of the supplied systems to confirm their good working order and / or conformity to the contract.

b. TRANSPORT COMMISSIONER and / or an outside agency nominated by TRANSPORT COMMISSIONER will conduct an acceptance test the hardware within a period of four weeks from the date of completion of installation and commissioning of hardware by the vendor. Acceptance test shall comprise of tests to verify conformity of technical requirements / specifications and performance. In case TRANSPORT COMMISSIONER is not satisfied with the above then, the vendor will upgrade / replace them with appropriate model. The exact details of acceptance test will be mutually decided after the installation of hardware.

VI) Health and performance monitoring features:

a. The proposed solution should be managed centrally through a single management console.

b. The management platform should be configured to proactively detect the health issues and service degradation / interruptions and should be able to create event / alerts to the relevant administrators through email, SMS etc.

VII) Warranty, Operation and maintenance support

The scope under warranty shall cover to provide services as described below.

a. All delivered items Hardware and software in this tender should be monitored and serviced in such a manner to ensure maximum uptime and performance levels. The guarantee / warranty should be highest nature extended by the OEM on the date of participation in the Tender (Necessary documentary evidence to be submitted).

b. The bidder will have to submit undertaking from all OEM's assuring availability of the equipment being sold would not be declared End of Sale (EoS) in the next 7 Years and that OEM shall supply similar or higher substitute in case EoS of equipment at no cost to TRANSPORT COMMISSIONER.

c. Also OEM should certify that the products being sold would be covered under Warranty / Support and support will be available for next five years from the date of installation at TRANSPORT COMMISSIONER.

d. Warranty of the hardware and subscription of the software will start from the date of Commissioning of last device.

e. Provide on-site comprehensive warranty for the supplied items – equipment / system / sub-systems (hardware / software) for a period of 5 years support on 24 x 7 basis from the date of acceptance. Defective equipment shall be replaced by the vendor at his own cost, including the cost of transport if any.

f. The hardware equipment (if any) should be guaranteed / warranted against all defects and failure and such guarantee / warranty shall include replacement of defective parts / equipment and / or repair of the same free of cost. In case of repetitive hardware failure (three times in a quarter), it shall be replaced by equivalent or higher new equipment by vendor at no extra cost to TRANSPORT COMMISSIONER. All warranty shall be onsite.

g. The bidder should confirm in their response that the support during warranty period would be carried out by the OEM for the respective equipment / peripheral. The bidder should also ensure that the highest level SLA (24 x 7) support with maximum resolution time of 4 hours is adhered to and this must be articulated in the bid response as well.

h. Any component in the Firewalls that are reported to be down on a given date should be replaced by substitute (of equivalent or higher configuration) in next business day in any location, the reporting will be through a telephonic message or any other mode as TRANSPORT COMMISSIONER may decide.

i. TRANSPORT COMMISSIONER reserves the right to levy / waive off penalty considering various circumstances at that point of time.

j. Warranty shall also cover the following:

   i. Installation / re-installation / maintenance / reconfiguration system software and other supplied software.

   ii. All system patches, critical hot fixed, upgrades, service packs etc. of the OS and all other software supplied must be made available free of cost.

   iii. Support for integration and update of infrastructure / network configuration and change management of the entire solution (existing as well as that procured as scope of this tender) to meet requirements.

   iv. Any change in the IP scheme, if required, limited to all the equipment installed at the TRANSPORT COMMISSIONER should be done.

VIII) Remote Support:

The bidder would be responsible to undertake Remote Support for a period of 5 Years. Remote Support will start from the date of warranty period starts.

The Remote support shall include but not limited to :

i. On-site, comprehensive, back-to-back from OEM for a period of 5 years from the date of starting warranty.

ii. Software updates and upgrades at no cost to the TRANSPORT COMMISSIONER.

iii. Configuration / re-configuration at the same location and / or any change of office location / premise as & when required to keep the equipment in working condition at free of cost.

iv. Traffic Analysis for different application / services as & when required / requested.

v. Co-ordinate with field staff & report progress of fault resolution to any branch office & Head office. Update should be given on every 4 hours during working days.

vi. The bidder must provide technical resources as and when required for coordinating with TRANSPORT COMMISSIONER staff for day to day operational issues as and when arises on supplied equipment such as QoS change request, IP accounting, monitoring / report generation etc., as required by TRANSPORT COMMISSIONER.

vii. Bidder should provide onsite preventive maintenance as per TRANSPORT COMMISSIONER Requirements.

viii. Bidder has to submit that escalation matrix from L1 to L3 level support for warranty Period.

IX) ANNEXURE

The items are to be delivered at the following locations (or) as informed by the department.

Sl.No	District Name	Office Name	Office Type
1	ALLURI SITHARAMA RAJU	RTA CHINTOOR	DTO
2		UNIT OFFICE PADERU	UNIT
3		CHECKPOST CHITTI	CP
4	ANAKAPALLI	RTA ANAKAPALLI	DTO
5		MVI OFFICE NARSIPATNAM	MVI
6	ANANTHAPURAM	RTA ANANTAPUR	DTO
7		UNIT OFFICE GUNTAKAL	UNIT
8		UNIT OFFICE RAYADURG	UNIT
9		UNIT OFFICE TADIPATRI	UNIT
10	ANNAMAYYA	MVI OFFICE PILER	MVI
11		UNIT OFFICE MADANAPALLE	UNIT
12		MVI OFFICE RAJAMPET	DTO
13		MVI OFFICE RAYACHOTI	MVI
14	BAPATLA	MVI OFFICE BAPATLA	DTO
15		UNIT OFFICE CHIRALA	UNIT
16	WEST GODAVARI	RTA BHIMAVARAM	DTO
17		UNIT OFFICE PALAKOLE	UNIT
18		UNIT OFFICE TADEPALLI GUDEM	UNIT
19		UNIT OFFICE TANUKU	UNIT
20	CHITTOOR	MVI OFFICE PALAMANER	MVI
21		UNIT OFFICE PUNGANUR	UNIT
22		RTA CHITTOOR	DTO
23		CHECKPOST NARAHARIPETA	CP
24		CHECKPOST PALAMANER	CP
25	ELURU	RTA ELURU	DTO
26		UNIT OFFICE JANGAREDDY GUDEM	UNIT
27		UNIT OFFICE NUZVID	UNIT
28		JANAMPET-TRACK	TRACK
29		CHECKPOST JEELUGUMILLI	CP
30	GUNTUR	RTA GUNTUR	DTO
31		UNIT OFFICE TENALI	UNIT
32		MVI OFFICE MANGALAGIRI	MVI

Sl.No	District Name	Office Name	Office Type
33	KAKINADA	MVI OFFICE PEDDAPURAM	MVI
34		RTA KAKINADA	DTO
35		UNIT OFFICE KATHIPUDI	UNIT
36		CHECKPOST KATHIPUDI	CP
37		RAJANGARAM-TRACK	TRACK
38	KONA SEEMA	RTA AMALAPURAM	DTO
39		UNIT OFFICE RAMACHANDRAPURAM	UNIT
40		UNIT OFFICE MANDAPETA	UNIT
41		UNIT OFFICE RAVULAPALEM	UNIT
42	KRISHNA	RTA GUDIWADA	RTO
43		RTA MACHILIPATNAM	DTO
44		UNIT OFFICE VUYYURU	UNIT
45	KURNOOL	RTA KURNOOL	DTO
46		UNIT OFFICE ADONI	UNIT
47		CHECKPOST KURNOOL	CP
48	MANYAM	MVI OFFICE PALAKONDA	MVI
49		MVI OFFICE PARVATHIPURAM	DTO
50		MVI OFFICE SALUR	MVI
51	NANDYAL	MVI OFFICE ATMAKUR-KURNOOL	MVI
52		MVI OFFICE DHONE	MVI
53		RTA NANDYAL	DTO
54		CHECKPOST SUNNIPENTA	CP
55	NTR	RTA NANDIGAMA	RTO
56		RTA VIJAYAWADA	DTO
57		UNIT OFFICE JAGGAYYAPET	UNIT
58		CHECKPOST GARIKAPADU	CP
59		CHECKPOST TIRUVURU	CP
60		GANNAVARAM-TRACK	TRACK
61	PALNADU	MVI CHILAKALURIPETA	MVI
62		MVI OFFICE MACHERLA	MVI
63		UNIT OFFICE PIDUGURALLA	UNIT
64		RTA NARASARAOPET	DTO
65		CHECKPOST DACHEPALLI	CP
66		CHECKPOST MACHERLA	CP
67	PRAKASAM	RTA PRAKASAM	DTO
68		UNIT OFFICE DARSI	UNIT
69		UNIT OFFICE MARKAPUR	UNIT
70	EAST GODAVARI	RTA RAJAHMUNDRY	DTO
71		UNIT OFFICE KOVVURU	UNIT

Sl.No	District Name	Office Name	Office Type
72	SPS NELLORE	MVI OFFICE ATMAKUR	MVI
73		MVI OFFICE KANDUKUR	MVI
74		RTA NELLORE	DTO
75		UNIT OFFICE KAVALI	UNIT
76	SRI BALAJI	RTA GUDUR	RTO
77		RTA TIRUPATI	DTO
78		MVI OFFICE SRIKALAHASTHI	MVI
79		UNIT OFFICE SULLURPET	UNIT
80		MVI OFFICE PUTTUR	MVI
81		CHECKPOST BHEEMUNIVARIPALEM	CP
82		CHECKPOST RENIGUNTA	CP
83	SRI SATYASAI	MVI OFFICE KADIRI	MVI
84		RTA HINDUPUR	DTO
85		CHECKPOST PENUKONDA	CP
86	SRIKAKULAM	RTA SRIKAKULAM	DTO
87		MVI OFFICE ITCHAPURAM	MVI
88		MVI OFFICE PALASA	MVI
89		MVI OFFICE TEKKALI	MVI
90		CHECKPOST PURUSHOTHAPURAM	CP
91	VISAKHAPATNAM	RTA VISHAKAPATNAM	DTO
92		RTA GAJUWAKA	RTO
93		GAMBHEERAM-TRACK	TRACK
94	VIZIANAGARAM	RTA VIZIANAGARAM	DTO
95	YSR KADAPA	MVI OFFICE BADVEL	MVI
96		MVI OFFICE PULIVENDULA	MVI
97		RTA CUDDAPAH	DTO
98		RTA PRODDUTUR	RTO
99	TC Office	STA	Head Office

Section E – Instructions to Bidders

E.1. Bidding Procedure:

Bid offers are to be made in three parts namely, "Prequalification bid", "Technical bid" and "Financial bid" and in the format given in bid document. All the documents are to be uploaded as per the documents in the corresponding section in eProcurement Website.

1. EMD details should be given in the "Pre-qualification bid".
2. Tenders shall be accepted only from those who have purchased the Bid Document.
3. All correspondence should be with APTS contact person.
4. A complete set of bidding documents to be purchased by interested bidders from APTS upon payment of the bid document price which is nonrefundable. Payment of bid document price should be by demand draft / cashier's cheque or certified cheque drawn in favor of "The Managing Director, Andhra Pradesh Technology Services Ltd." and payable at Vijayawada (India) not later than 1hour before bid closing date & time or through online payment.
5. APTS Bank Account details for online payment of tender document fee are:
    a. Bank A/c. No.: 52082155102
    b. IFSC Code: SBIN0003055
    c. Bank Name: State Bank of India, Labbipet, Vijayawada
    d. MICR Code: 520002007

E.2. Pre-qualification bid:

It shall include the following information about the firm and its proposal.

1. General information on the bidder's company in Form P-1
2. Details of Turnover in Form P-2
3. List of major customers in support of turnover in Form P-3
4. Details of service centers in AP in Form P-4
5. Declaration regarding clean track record in Form-P5
6. Valid Certificates like BIS, ISO, Microsoft etc.
7. Manufacturer's authorization to participate in bidding process apart from such other documents like authorization certificate for dealing in the products for which bid is submitted. (However this will not apply to Manufacturers) as per Annexure III.

E.3. Technical Bid:

1. Technical Compliance Statement with Make, Model, Specifications mentioned in tender document and offered specifications in Form T-1.
2. Check list in Form T-2
3. Detailed technical documentation, reference to various industry standards to which the products/services included in vendor's offer conform, and literature concerning the proposed solution
4. Other information, if any required in the bid document

E.4. Financial bid:

The financial bid should provide cost calculations corresponding to unit price of each item of the respective schedules in Cost sheets.

E.5. Pre-bid Meeting:

Bidders who purchased bid document only will be allowed to participate in the pre-bid meeting to seek clarifications on the bid, if any. The pre-bid meeting will be conducted either in physical presence mode or through online virtual meeting tools. Interested bidders should send email request to APTS contact person for communicating the online meeting link.

Section F – Bid Evaluation Procedure

F.1. Bid evaluation procedure:

Bids would be evaluated item wise/schedule wise. Technical bid documentation should be in the prescribed format. If a vendor has any comment to offer about the procedural aspects of this tender, it should be intimated to APTS during the pre-bid meeting. In case the schedule or procedure of tender processing is revised, the same shall be communicated by telephone, fax, courier or e-mail as the case may be to all the vendors who have paid the tender document fee.

F.2. Opening of bids:

1. Bids will be opened on the e-Procurement website at the scheduled time & date as specified.

2. APTS contact person shall open the pre-qualification bid, after the bid closing time and list them for further evaluation. After evaluation of Pre-Qualification bids, the technical bids of only those bidders who qualify in Pre-qualification will be opened. Similarly, the financial bids of only those bidders who qualify in technical evaluation will be opened.

F.3. EMD Validity:

The EMD will be scrutinized first for the amount and validity period. The bids submitted with required EMD amount and validity only be considered for the evaluation. The bids submitted with insufficient EMD amount/validity will be treated as disqualified bids and those bids will not be considered for further evaluation.

F.4. Pre-qualification bid documentation:

The Pre-qualification bid documentation shall be evaluated in two sub-steps.

a) Firstly, the documentation furnished by the vendor shall be examined prima facie to see if the technical skill base and financial capacity and other vendor attributes claimed therein are consistent with the needs of this project.
b) In the second step, APTS may ask vendor(s) for additional information, visit to vendors site and/or arrange discussions with their professional, technical faculties to verify claims made in Pre-qualification bid documentation.

F.5. Technical bid documentation:

Technical bid documentation shall be evaluated in two sub-steps.

a) Firstly, the documentation furnished by the vendor shall be examined prima facie to see if the product /services offered, technical skill base and financial capacity and other vendor attributes claimed therein are consistent with the needs of this project.
b) In the second step, APTS may ask vendor(s) for additional information, visit to vendors site and/or arrange discussions with their professional, technical faculties to verify claims made in technical bid documentation.

F.6. Award Criterion:

Final choice of firm to execute the project shall be made on the basis of conformity to technical specifications, appropriateness of the product offered, capability of bidder to execute and service the project and appropriateness of financial offer from the point of view of cost-effectiveness over the entire maintenance period for the product/services.

Managing Director, APTS

Section G – General Instructions to Bidders

G.1. Definitions:

1. **Tender call or invitation for bids** means the detailed notification seeking a set of solution(s), service(s), materials or any combination of them.
2. **Specifications** means the functional and technical specifications or statement of work, as the case may be.
3. **Firm** means a company, authority, co-operative or any other organization incorporated under appropriate statute as is applicable in the country of incorporation.
4. **Bidder** means any firm offering the solution(s), service(s) and/or materials required in the tender call. The word vendor when used in the pre award period shall be synonymous with bidder and when used after award of the contract shall mean the successful bidder with whom APTS/Department signs the contract for rendering of goods and services.
5. **Pre-qualification and Technical bid** means that part of the offer that provides information to facilitate assessment by APTS, professional, technical and financial standing of the bidder, conformity to specifications etc.
6. **Financial Bid** means that part of the offer, that provides price schedule, total project costs etc.
7. **Three Part Bid** means the pre-qualification bid, technical and financial bids submitted in Physical to APTS / through eProcurement portal.
8. **Two Part Bid** means the Technical bid (including Pre-Qualification) and financial bids submitted in physical to APTS / through eProcurement portal and their evaluation is sequential.
9. **Composite Bid** means a bid in which the technical and financial parts are combined into one, but their evaluation is sequential.
10. **Goods and Services** mean the solution(s), service(s), materials or a combination of them in the context of the tender call and specifications.
11. **The word goods** when used singly shall mean the hardware, firmware component of the goods and services.
12. **Maintenance Period** means period mentioned in bid document for maintaining the systems beyond warranty period.
13. **Prime Bidder** means a company part of the consortium wholly responsible for contractual obligations and act as Single Point of Contact for the contract management.

G.2 General Eligibility

1. This invitation for bids is open to all firms both from within and outside India, who are eligible to do business in India under relevant Indian laws as is in force at the time of bidding subject to meeting the pre-qualification criterion.
2. Bidders marked/considered by APTS to be ineligible to participate for non-satisfactory past performance, corrupt, fraudulent or any other unethical business practices shall not be eligible.
3. Bidder/Consortium Member debarred/ blacklisted by any Central or State Govt. / Quasi –Govt. Departments or organizations as on bid calling date for non-satisfactory past performance, corrupt, fraudulent or any other unethical business practices shall not be eligible.

4. Breach of general or specific instructions for bidding, general and special conditions of contract with APTS or any of its user organizations may make a firm ineligible to participate in bidding process.

G.3 Bid forms

1. Wherever a specific form is prescribed in the bid document, the bidder shall use the form to provide relevant information. If the form does not provide space for any required information, space at the end of the form or additional sheets shall be used to convey the said information.
2. For all other cases the bidder shall design a form to hold the required information.

G.4 Cost of bidding

1. The bidder shall bear all costs associated with the preparation and submission of its bid, and APTS will in no case be responsible for those costs, regardless of the conduct or outcome of the bidding process.
2. Bidder is expected to examine all instructions, forms, terms, and specifications in the bidding documents. Failure to furnish all information required by the bidding documents or to submit a bid not substantially responsive to the bidding documents in every respect will be at the bidder's risk and may result in the rejection of its bid.

G.5 Clarification of bidding documents

1. A prospective vendor requiring any clarification of the bidding documents may notify APTS contact person. Written copies / e-mail of the APTS response (including an explanation of the query but without identifying the source of inquiry) will be sent to all prospective bidders that have received the bidding documents.
2. The concerned person will respond to any request for clarification of bidding documents which it receives no later than bid clarification date mentioned in the notice prior to deadline for submission of bids prescribed in the tender notice. No clarification from any bidder shall be entertained after the close of date and time for seeking clarification mentioned in tender call notice. It is further clarified that APTS shall not entertain any correspondence regarding delay or non-receipt of clarification from APTS.

G.6 Amendment of bidding documents

1. At any time prior to the deadline for submission of bids, APTS, for any reason, whether at its own initiative or in response to a clarification requested by a prospective bidder, may modify the bidding documents by amendment.
2. All prospective bidders those who have received the bidding documents will be notified of the amendment and such modification will be binding on all bidders.
3. In order to allow prospective bidders reasonable time in which to take the amendment into account in preparing their bids, the APTS, at its discretion, may extend the deadline for the submission of bids.

G.7 Period of validity of bids

1. Bids shall remain valid for the days or duration specified in the bid document, after the date of bid opening prescribed by APTS. A bid valid for a shorter period shall be rejected as non-responsive.

2. In exceptional circumstances, the APTS may solicit the bidders' consent to an extension of the period of validity. The request and the responses thereto shall be made in writing. The bid security shall also be suitably extended. A bidder granting the request will not be permitted to modify its bid.

G.8 Submission of bids

The bidders shall submit all the bids i.e., Pre-Qualification, Technical and Financial Bids on e-Procurement website only.

G.9 Deadline for submission of bids

1. Bids must be submitted on e-procurement website not later than the bid submission date and time specified in the tender call notice.
2. The APTS may, at its discretion, extend this deadline for the submission of bids by amending the tender call, in which case all rights and obligations of the APTS and bidders previously subject to the deadline will thereafter be subject to the deadline as extended.

G.10 Late bids

Any bid not submitted through online, before bid closing time will be rejected.

G.11 Modification and withdrawal of bids

1. No bid can be modified subsequent to the deadline for submission of bids.
2. No bid can be withdrawn in the interval between the deadline for submission of bids and the expiration of the period of bid validity. Withdrawal of a bid during this interval will result in the forfeiture of its bid security (EMD).

G.12 General Business information:

The bidder shall furnish general business information to facilitate assessment of its professional, technical and commercial capacity and reputation.

G.13 Bid security i.e. Earnest Money Deposit (EMD)

1. The bidder shall furnish, as part of its bid, a bid security for the amount specified in the tender call notice.
2. The bid security is required by APTS to:
    a. Assure bidder's continued interest till award of contract and
    b. Conduct in accordance with bid conditions during the bid evaluation process.
3. The bid security shall be in Indian rupees and shall be a bank guarantee or an irrevocable letter of credit or cashier's certified check, issued by a reputable bank scheduled in India and having at least one branch office in Vijayawada.
4. Unsuccessful bidder's bid security will be discharged or returned as promptly as possible but not later than thirty (30) days after the expiration of the period of bid validity prescribed by APTS.
5. The successful bidder's bid security will be discharged upon the bidder signing the contract, and furnishing the performance security,
6. The bid security may be forfeited:
    a. if a bidder withdraws its bid during the period of bid validity or

b. in the case of a successful bidder, if the bidder fails:
    i. to sign the contract in time; or
    ii. to furnish performance security.

G.14. Preparation of Pre-qualification bid

It shall contain of the following parts:

1. General business information
2. Turnover details
3. Major clients' details
4. Service center details
5. Bid security (EMD)
6. Any other relevant information

G.15 Preparation of technical bid

It shall consist of the following parts.

1. Technical documentation – confirmation to technical specifications etc.
2. Plan for in lab proof of concept, if required in tender call.
3. Plan for field demonstration if required in tender call
4. Detailed technical documentation, reference to various industry standards to which the goods and services included in vendor's offer conform, and other literature concerning the proposed solution. In particular, the vendors should identify areas in which their solution conforms to open standards and areas that are proprietary in nature. Justification about proprietary components in terms of functionality and performance should be given.
5. A statement about appropriateness of the product design and solution plan for operating conditions in India, including physical, infrastructure and human factors.
6. In the case of a bidder offering to supply goods under the contract which the bidder did not manufacture or otherwise produce, the bidder has been duly authorized by the good's manufacturer or producer to supply the goods in India.
7. A statement of the serviceable life of goods and services offered by the firm. Available sources of maintenance and technical support during the serviceable life. Available sources of spare parts, special tools, etc. Necessary for the proper and continuing functioning of the goods and services, for the serviceable life.

G.16 Preparation of financial bid

Overview of financial bid

The financial bid should provide cost calculations corresponding to each component of the project.

1. Bid prices
    a. The bidder shall indicate the unit prices (where applicable) and the total bid price of the goods/services it proposes to supply under the contract.
    b. The bidder shall indicate Basic Prices and taxes, duties etc. (if required) in the form prescribed.
    c. Bidder's separation of price components will be solely for the purpose of facilitating the comparison of bids by APTS and will not in any way limit the purchaser's right to contract on any of the terms offered.

d. Prices quoted by the bidder shall be fixed during the bidder's performance of the contract and not subject to variation on any account unless otherwise specified in the tender call. A bid submitted with an adjustable price quotation will be treated as non-responsive and will be rejected.

2. Bid currency:

Prices shall be quoted in Indian rupees.

Section H – Standard Procedure for opening and evaluation of bids

H.1.Outline of bid evaluation procedure

1. The bid opening and evaluation process will be sequential in nature. Means that bidder must qualify a particular stage to be eligible for next stage. Immediately after the closing time, the APTS contact person shall open the Pre-qualification bids and list them for further evaluation.
2. If it is a manual tender- the Technical and financial bid covers shall be listed and put into a bag to be sealed according to APTS procedure. The sealed bag of technical and financial bids shall be in custody of a designated officer for opening after evaluation of Pre-qualification bids. Thereafter, Technical bids of qualified bidders will be opened, keeping financial bid in sealed bag. Finally, financial bids of those bidders will be opened who are short listed in technical evaluation.
3. In case of composite bid – technical and financial bids combined together, first technical evaluation will be done followed by financial evaluation of only those bids, which have qualified in technical evaluation.
4. Any participating vendor may depute a representative to witness these processes.
5. The standard procedure, described here will stand appropriately modified, in view of special procedures of bid evaluation as mentioned in tender call or elsewhere in this bid document or APTS may deviate from these in specific circumstances if it feels that such deviation are unavoidable, or will improve speed of processing and consequent project execution.

H.2. General Guidelines for bid opening and evaluation:

Bids will be in three parts (pre-qualification, technical and financial) or two parts (PQ&Technical bid together and financial) or composite bid (technical and financial bid together) as indicated in the tender call. For three part bids there will be three bid opening events, in two part bid there will be two bid opening events and in case of composite bids there will be only one bid opening event. Following guidelines will generally be followed by APTS officers at each such event. However, APTS may deviate from these in specific circumstances if it feels that such deviation are unavoidable, or will improve speed of processing and consequent project execution.

H.3 Opening of bids

Bids will be opened on the e-Procurement web site at the scheduled time & date.

1. The bidders names, bid modifications or withdrawals, discounts, and the presence or absence of requisite bid security and such other details as the APTS officer at his/her discretion, may consider appropriate, will be announced at the opening. No bid shall be rejected at bid opening, except for late bids, which shall be returned unopened.
2. Bids that are not opened and read out at bid opening shall not be considered further for evaluation, irrespective of the circumstances. Withdrawn bids will be returned unopened to the bidders.

H.4. Preliminary examination of Bids

1. Preliminary scrutiny will be made to determine whether they are complete, whether any computational errors have been made, whether required sureties have been furnished, whether the documents have been properly signed, and whether the bids are generally in order.
2. Arithmetical errors will be rectified on the following basis. If there is a discrepancy between the unit price and the total price that is obtained by multiplying the unit price and quantity, the unit price shall prevail, and the total price shall be corrected. If the vendor does not accept the correction of the errors, its bid will be rejected, and its bid security may be forfeited. If there is a discrepancy between words and figures, the amount in words will prevail.
3. APTS may waive any minor informality, nonconformity or irregularity in a bid which does not constitute a material deviation, provided such waiver does not prejudice or affect the relative ranking of any bidder.
4. Prior to the detailed evaluation, APTS will determine the substantial responsiveness of each bid to the bidding documents. For purposes of these clauses, a substantially responsive bid is one which conforms to all the terms and conditions of the bidding documents without material deviations.
5. If a bid is not substantially responsive, it will be rejected by the APTS and may not subsequently be made responsive by the bidder by correction of the nonconformity.

H.5. Clarification of bids

During evaluation of the bids, APTS may, at its discretion, ask the bidder for clarification of its bid.

Any Queries / representations should be submitted within 2 days from the date of publishing of the tender. APTS reserves the right to consider or not to consider the Queries received from the bidders.

H.6.Evaluation of Pre – qualification bids

Pre – qualification bid documentation shall be evaluated in two sub-steps.

1. Firstly, the documentation furnished by the vendor will be examined prima facie to see if the technical skill base and financial capacity and other vendor attributes claimed therein are consistent with the needs of this project.
2. In the second step, APTS may ask vendor(s) for additional information, visit to vendors site and/or arrange discussions with their professional, technical faculties to verify claims made in technical bid documentation.

H.7. Evaluation of technical bids.

Technical bid documentation shall be evaluated in two sub-steps.

1. Firstly, the documentation furnished by the vendor will be examined prima facie to see if the offer made, technical skill base and financial capacity and other vendor attributes claimed therein are consistent with the needs of this project.
2. In the second step, APTS may ask vendor(s) for additional information, visit to vendors site and/or arrange discussions with their professional, technical faculties to verify claims made in technical bid documentation.

H.8. In lab proof of concept

The lab proof of concept on demand may be organized either in APTS or in the vendor's lab by mutual discussion. In case it is organized in APTS lab, APTS would make available generic hardware for this purpose. Application specific hardware and software will have to be brought in by the vendor.

H.9. Field demonstration

APTS will identify a part or segment of the proposed project site. The concerned bidder, on demand, should be able to demonstrate functional requirements as described in the specifications.

H.10. Evaluation of financial bids

Financial bids of those vendors who satisfy all phases of the pre-qualification and technical bid and corresponding to chosen technical bid choices will only be opened. All other financial bids will be ignored. APTS will assess the nature of financial offers and may pursue any or all of the options mentioned under financial bid APTS may at its discretion discuss with vendor(s) available at this stage to clarify contents of financial offer.

1. Bids will be evaluated item wise in each schedule.
2. ***Evaluation of Financial Bids will be including taxes.***

H.11. Evaluation and comparison of financial bids

1. Evaluation of financial bids will exclude and not take into account any offer not asked for or not relevant to the present requirements of user.
2. Evaluation of financial bid will take into account, in addition to the basic bid price, one or more of the following factors
    a. The projected costs for the entire contract period;
    b. Past track record of bidder in supply/ services and
    c. Any other specific criteria indicated in the tender call and/or in the specifications.

H.12. Performance and productivity of the equipment

Bidders shall state the guaranteed performance or efficiency in response to the specifications.

H.13. Contacting APTS

1. Bidder shall not approach APTS officers outside of office hours and / or outside APTS office premises, from the time of the tender call notice to the time the contract is awarded.
2. Any effort by a bidder to influence APTS officers in the decisions on bid evaluation, bid comparison or contract award may result in rejection of the bidder's offer and bidder may also be marked as ineligible for future bids. If the bidder wishes to bring additional information to the notice of the APTS, it should do so in writing.

H.14. APTS/Department right to vary quantities at time of award

1. APTS/Department reserves the right at the time of award to increase or decrease the quantity, as indicated in tender call, from the quantity of goods and services originally specified in the specification without any change in unit price or other terms and conditions.

2. APTS/Department reserves the right to place the repeat orders at the quoted price, in addition to the Quantity for which bid has been called for. However, this condition will not create any right to the bidder to demand such repeat order. During the validity of the contract period thereof, the bidder should be ready to supply any no. of devices as requested.

H.15. APTS' right to accept any bid and to reject any or all bids.

1. Any deviations in the formats may make the bid liable for rejection.
2. APTS reserves the right to modify / extend / cancel the tender at any point of time without giving any prior notice / any reasoning.

H.16. Notification of award

1. Prior to expiration of the period of bid validity, APTS will notify the successful bidder in writing, that its bid has been accepted.
2. Upon the successful bidder's furnishing of performance security, APTS will promptly notify each unsuccessful bidder and will discharge its bid security.

H.17. Signing of contract

1. At the same time as the APTS notifies the successful bidder that its bid has been accepted, the APTS/Department will send the bidder the Contract Form provided in the bidding documents, incorporating all agreements between the parties.
2. On receipt of the Contract Form, the successful bidder shall sign and date the contract and return it to the APTS/Department.

H.18. Performance security

1. On receipt of notification of award from the APTS, the successful bidder shall furnish the performance security in accordance with the conditions of contract, in the performance security form provided in the bidding documents or in another form acceptable to the APTS/Department.
2. Failure of the successful bidder to sign the contract, proposed in this document and as may be modified, elaborated or amended through the award letter, shall constitute sufficient grounds for the annulment of the award and forfeiture of the bid security, in which event the APTS/Department may make the award to another bidder or call for new bids.

H.19. Corrupt, fraudulent and unethical practices

1. **"Corrupt practice"** means the offering, giving, receiving or soliciting of anything of value to influence the action of a public official in the process of contract execution and
2. **"Fraudulent practice"** means a misrepresentation of facts in order to influence a procurement process or the execution of a contract to detriment of the purchaser, and includes collusive practice among Bidders (prior to or after bid submission) designed to establish bid prices at artificial non-competitive levels and to deprive the Purchaser of the benefits of free and open competition:

3. **"Unethical practice"** means any activity on the part of bidder, which try to circumvent tender process in any way. Unsolicited offering of discounts, reduction in financial bid amount, upward revision of quality of goods etc after opening of first bid will be treated as unethical practice.
4. APTS/Department will reject a proposal for award and also may debar the bidder for future tenders in APTS/Department, if it determines that the bidder has engaged in corrupt, fraudulent or unethical practices in competing for, or in executing a contract.

H.20. Negotiation

APTS reserves its right to negotiate with the lowest quoted bidder including technical specifications.

Section I – General Conditions of Proposed Contract (GCC)

I.1. Definitions

In this contract, the following terms shall be interpreted as indicated. Terms defined in general instructions to bidders section shall have the same meaning.

1. **"Contract"** means the agreement entered into between the APTS/Department and the vendor, as recorded in the contract form signed by the parties, including all attachments and appendices thereto and all documents incorporated by reference therein;
2. **"Contract Price"** means the price payable to the vendor under the contract for the full and proper performance of its contractual obligations;
3. **"Incidental Services**" means those services ancillary to the supply of the goods and services, such as transportation and insurance, and any other incidental services, such as installation, commissioning, provision of technical assistance, training and other such obligations of the vendor covered under the contract;
4. **"GCC"** means the general conditions of contract contained in this section.
5. **"SCC"** means the special conditions of contract if any.
6. **"APTS"** means the Andhra Pradesh Technology Services Ltd.
7. **"Purchaser/ User"** means ultimate recipient of goods and services
8. **"Vendor or Bidder"** means the individual or firm supplying the goods and services
9. under this contract.
10. **"Project Site"**, where applicable, means the place(s) where goods/services are to be made available to user.
11. **"Day"** means calendar day.
12. **"Up Time"** means the time period when specified services with specified technical and service standards are available to user(s)
13. **"Down Time"** means the time period when specified services with specified technical and service standards are not available to user(s).

I.2 Application

These general conditions shall apply to the extent that they are not superseded by provisions of other parts of the contract.

I.3 Standards

The goods supplied under this contract shall conform to the standards mentioned in the specifications, and, when no applicable standard is mentioned, the authoritative standards appropriate to the goods' country of origin shall apply. Such standard shall be the latest issued by the concerned institution.

I.4 Use of documents and information

1. The vendor shall not, without prior written consent from APTS, disclose/share/use the bid document, contract, or any provision thereof, or any specification, plan, drawing, pattern, sample or information furnished by or on behalf of the APTS in connection therewith, to any person other than a person employed by the vendor in the performance of the contract. Disclosure to any such employed person shall be made in confidence and shall extend only so far as may be necessary for purposes of such performance.

2. The Vendor shall not, without prior written consent of APTS, make use of any document or information made available for the project, except for purposes of performing the Contract.
3. All project related document (including this bid document) issued by APTS, other than the contract itself, shall remain the property of the APTS and shall be returned (in all copies) to the APTS on completion of the Vendor's performance under the contract if so required by the APTS.

I.5. User license and patent rights

1. The Vendor shall provide licenses for all software products, whether developed by it or acquired from others. In the event of any claim asserted by a third party for software piracy, the vendor shall act expeditiously to extinguish such claim. If the vendor fails to comply and the APTS/Department is required to pay compensation to a third party resulting from such software piracy, the vendor shall be responsible for compensation including all expenses, court costs and lawyer fees. The APTS/Department will give notice to the vendor of such claim, if it is made, without delay.
2. The Vendor shall indemnify the purchases against all third party claims of infringement of patent, trademark or industrial design rights arising from use of the goods, software package or any part thereof.

I.6. Performance security

1. On receipt of notification of award, the Vendor shall furnish performance security to APTS/Department in accordance with bid document requirement.
2. The proceed of the performance security shall be payable to the APTS/Department as compensation for any loss resulting from the supplier's failure to complete its obligations under the contract.
3. The performance security shall be denominated in Indian rupees or in a freely convertible currency acceptable to APTS/Department and shall be in one of the following forms:
    a. A bank guarantee or an irrevocable letter of credit, issued by a reputed bank located in India with at least one branch office in Vijayawada, in the form provided in the bidding document or another form acceptable to the APTS/Department; or
    b. A cashier's cheque or banker's certified cheque or crossed demand draft or pay order drawn in favor of the APTS/Department.
4. The performance security will be discharged by the APTS/Department and returned to the Vendor not later than thirty (30) days following the date of completion of all formalities under the contract and if activities, post warranty, by the Vendor is envisaged, following receipt of a performance guarantee for annual maintenance as per bid document.
5. In the event of any contract amendment, the vendor shall, within 15 days of receipt of such amendment, furnish the amendment to the performance security, rendering the same valid for the duration of the Contract.

I.7. Manuals and drawings

1. Before the goods and services are taken over by the user, the Vendor shall supply operation and maintenance manuals, (together with drawings of the goods and services where applicable).
2. The Vendor shall provide complete technical documentation of hardware, firmware, all subsystems, operating systems, compiler, system software and the other software.
3. The manuals and drawings wherever applicable shall be in English or Telugu.
4. At least one set of the manuals should be supplied for each installation sites.
5. Unless and otherwise agreed, the goods and services shall not be considered to be completed for the purpose of taking over until such manuals and drawings have been supplied to the user.

I.8. Inspection and acceptance tests

1. Inspection and tests prior to shipment of Goods and at final acceptance are as follows:
   a. Inspection of the goods shall be carried out to check whether the goods are in conformity with the specifications mentioned in the bid document. Following broad test procedure will generally be followed for inspection and testing of hardware and firm wares. The vendor will dispatch the goods to the ultimate consignee after internal inspection testing along with the supplier's inspection report, manufacturer's warranty certificate. The APTS/Department will test the equipment after completion of the installation and commissioning at the site of the installation. (If site preparation is not included in the tender call or specification, the vendor should furnish all details of the site requirement to the APTS/Department sufficiently in advance so as to get the works completed before receipt of the equipment.)
   b. The Inspections and tests, at the discretion of APTS/Department, may be conducted on the premises of the Vendor, at point of delivery, and / or at the good's final destination. If conducted on the premises of the Vendor, all reasonable facilities and assistance, including access to drawings and production data, shall be furnished to the inspectors at no charge to the APTS/Department.
   c. Should any inspected or tested goods fail to conform to the specifications the APTS/Department may reject the goods, and the vendor shall either replace the rejected goods or make alterations necessary to meet specification requirements free of cost to the APTS/user.
   d. APTS/Department right to inspect, test and, where necessary reject the goods after the goods' arrival at user's site shall in no way be limited or waived by reason of the goods having previously been inspected, tested and passed by the APTS/Department or its representative prior to the goods shipment from the country of origin.
   e. Nothing in this clause shall in any way release the vendor from any warranty or other obligations under this contract.

f. The acceptance test will be conducted by the APTS/Department, their consultant or any other person nominated by the APTS/Department, at its option. There shall not be any additional charges for carrying out acceptance tests. Any reduction in functional requirements, and performance specifications shall be ground for failure. Any malfunction, partial or complete failure of any part of hardware, firmware or bugs in the software shall be grounds for failure of acceptance test. All the software should be complete, and no missing modules / sections will be allowed. The vendor shall maintain necessary log in respect of the results of the tests to establish to the entire satisfaction of the APTS/Department, the successful completion of the test specified. An average uptake efficiency of 97% for the duration of test period (7 days) shall be considered as satisfactory.

g. In the event of the hardware and software failing to pass the acceptance test, A period not exceeding two weeks will be given to rectify the defects and clear the acceptance test, failing which the APTS/Department reserves the rights to get the Equipment replaced by the vendor at no extra cost to the APTS/Department.

I.9. Acceptance certificates

On successful completion of acceptability test, receipt of deliverables etc, and after APTS/Department is satisfied with the working of the system, the acceptance certificate signed by the vendor and the representative of the APTS/Department will be issued. The date on which such certificate is signed shall be deemed to be the date of successful commissioning of the systems.

I.10. Packing

1. The vendor shall provide such packing of the goods as is required to prevent their damage or deterioration during transit to their final destination. The packing shall be sufficient to withstand, without limitation, rough handling during transit and exposure to extreme temperature, salt and precipitation during transit and open storage. Packing case size and weights shall take into consideration, where appropriate, the remoteness of the goods' final destination and the absence of heavy handling facilities at all points in transit.
2. The packing, marking and documentation within and outside the packages shall comply strictly with such special requirements as shall be expressly providedfor in the contract, including additional requirements, if any, specified in SCC, and in any subsequent instructions ordered by the APTS/Department.

I.11. Delivery and documents

Delivery of the goods/services shall be made by the vendor in accordance with the terms specified in the Schedule of requirements. The details of shipping and / or other documents to be furnished and submitted by the vendor are specified below.

A) For Goods supplied from abroad:

1. Within 24 hours of shipment, the Vendor shall notify the APTS/Department and the Insurance Company by cable or telex or fax full details of the shipment including contract number, description of goods, quantity, the vessel, the bill of lading number and date, port of loading, date of shipment, port of discharge, etc. The Vendor shall mail the following documents to the APTS/Department, with a copy to the Insurance Company.

2. Four copies of supplier's invoice showing goods description, quantity, unit price and total amount;
3. 4 copies of packing list identifying contents of each package;
4. Insurance certificate; Manufacturer's/Supplier's warranty certificate;
5. Inspection certificate, issued by the nominated inspection agency and
6. The Supplier's factory inspection report; and Certificate of origin.
7. The above documents shall be received by the APTS/Department at least one week before arrival of Goods at the port or place of arrival and, if not received, the Vendor will be responsible for any consequent expenses.

B) For Goods from within India:

Upon delivery of the goods to the user, the vendor shall notify the APTS/Department and mail the following documents to the APTS/Department:

1. Four copies of the Vendor invoice showing goods description, quantity, unit price total amount;
2. Delivery note, or acknowledgement of receipt of goods from the user;
3. Manufacturer's or Supplier's warranty certificate;
4. Inspection Certificate issued by the nominated inspection agency, and the Supplier's factory inspection report.
5. Certificate of Origin;
6. Insurance policy;
7. Excise gate pass Octroi receipts wherever applicable duly sealed indicating payments made; and
8. Any of the documents evidencing payment of statutory taxes.
9. The above documents shall be received by the APTS/Department before arrival of the Goods (except deliver note and where it is handed over to the user with all documents) and if not received, the vendor will be responsible for any consequent expenses.

I.12.Insurance

1. It is suggested that the goods supplied under the contract shall be fully insured in a freely convertible currency against loss or damage incidental to manufacture or acquisition, transportation, storage, and delivery up to user site.
2. The insurance should be for replacement value from "Warehouse to warehouse (final destination)" on "All Risks" valid upto 3 months till completion of delivery, installation and commissioning.

I.13. Transportation

Transport of the goods to the project site(s) shall be arranged by the vendor at his cost.

I.14. Hardware Installation

The vendor is responsible for all unpacking, assemblies, installations and connecting to power supplies. The vendor will test all hardware operations and accomplish all adjustments necessary for successful and continuous operation of the computer hardware at all installation sites.

I.15. Incidental services

The Vendor may be required to provide any or all the following services, including additional services:

1. Performance or supervision or maintenance and/or repair of the supplied goods and services, for a period of time agreed by the parties, provided that this service shall not relieve the Vendor of any warranty obligations under this Contract, and
2. Training of APTS and/or its user organization personnel, at the Vendor's site and / or on-site, in assembly, start-up, operation, maintenance and/or repair of the supplied goods and services.
3. Prices charged by the Vendor for the preceding incidental services, if any, should be indicated separately (if required), and same will be mutually negotiated separately.

I.16. Spare parts

1. The Vendor may be required to provide any or all of the following materials, notifications and information pertaining to spare parts manufactured or distributed by the Vendor.
2. Such spare parts as the APTS/Department may elect to purchase from the Vendor, provided that this election shall not relieve the Vendor of any warranty obligations under the contract and
3. In the event of termination of production of the spare parts, an advance notification to the APTS/Department of the pending termination, in sufficient time to permit the APTS to procure needed requirements and
4. The Vendor shall ensure availability of spares in stock at his nearest service centre for immediate delivery such spare parts as: (a) are necessary for a minimum of 5 years of operation after installation at the Purchaser's sites (b) are necessary to comply with specifications.

I.17. Warranty

1. The Vendor warrants that the goods and services supplied under the contract are new, unused, of the most recent or current models, and that they incorporate all recent improvements in design and materials unless provided otherwise in the contract. The Vendor further warrants that all goods and services supplied under this contract shall have no defect arising from design, materials or workmanship or from any act or omission of the Vendor, that may develop under normal use of the supplied goods in the conditions prevailing in the country of final destination.
2. The warranty period shall be as stated in bid document. The Vendor shall, in addition, comply with the performance guarantees specified under the contract. If, for reasons attributable to the Vendor, these guarantees are not attained in whole or in part, the Vendor shall, make such changes, modifications, and/or additions to the goods or any part thereof as may be necessary in order to attain the contractual guarantees specified in the contract at its own cost and expenses and to carry out further performance tests.
3. The equipment supplied should achieve required up time.
4. APTS/Department shall promptly notify the Vendor in writing of any claims arising under this warranty.

5. Upon receipt of such notice, the Vendor shall, within the period specified in GCC and with all reasonable speed, repair or replace the defective goods and services or parts thereof, without costs to the user.
6. If the Vendor, having been notified, fails to remedy the defect(s) within a reasonable period, the APTS/Department may proceed to take such remedial action as may be necessary, at the vendor's risk and expense and without prejudice to any other rights which the APTS /Department may have against the Vendor under the contract.

I.18. Maintenance service

1. Free maintenance services including spares shall be provided by the vendor during the period of warranty. User, at its discretion may ask the vendor to provide maintenance services after warranty period, i.e. Annual maintenance and repairs of the system at the rates indicated by bidder in its proposal and on being asked so, the vendor shall provide the same. The cost of annual maintenance and repairs cost (after warranty period), which will include cost of spares replaced, shall be paid in equal quarterly installments at the end of each quarter.
2. The maximum response time for maintenance complaint from any of the destination (i.e. time required for supplier's maintenance engineers to report to the installations after a request call/telegram is made or letter is written) shall not exceed 48 hours.
3. The vendor will accomplish preventive and breakdown maintenance activities to ensure that all hardware, and firmware execute without defect or interruption for at least required up time.
4. In case up time is less than the stipulated up time, penalty as indicated in the bid document shall be imposed on the vendor.
5. The amount of penalty if any, will be recovered at source from the performance guarantee during the warranty or from annual maintenance charges payable as the case may be.

I.19. Payment

1. The vendor's request(s) for payment shall be made to the APTS / Department in writing, accompanied by an invoice describing, as appropriate, the goods/service delivered/ performed.
2. Payments shall be made promptly by the APTS/User Department, but in no case later than (30) days after submission of a valid invoice or claim by the vendor.
3. The currency of payment will be Indian rupees.
4. Payment shall be made as indicated in Bid document.
5. The annual maintenance and repair cost as per separate agreement if any, shall be paid in equal quarterly installments at the end of each quarter as per the rates quoted and agreed.
6. Payment will be made through Cheque/online.

I.20. Prices

Prices charged by the Vendor for goods delivered and services performed under the contract shall not vary from the prices quoted by the Vendor in its bid, with the exception if any price adjustments authorized in special conditions of contract or in the request for bid validity extension, as the case may be.

I.21. Change orders

APTS/Department may, at any time, by written order given to the Vendor, make changes within the general scope of the Contract in any one or more of the following:

1. Drawing, designs, or specifications, where Goods to be supplied under the Contract are to be specifically manufactured for the APTS/Department;
2. The method of shipment or packing;
3. The place of delivery and/or the services to be provided by the Vendor.
4. If any such change causes an increase or decrease in the cost of, or the time required for, the vendor's performance of any provisions under the contract, an equitable adjustment shall be made in the contract price or delivery schedule, or both, and the contract shall accordingly be amended.
5. Any claims by the Vendor for adjustment under this clause must be asserted within thirty (30) days from the date of the Vendor's receipt of the change order.

I.22. Contract amendment

No variation in or modification of the terms of the Contract shall be made except by written amendment signed by the parties.

I.23. Assignment

The Vendor shall not assign, in whole or in part, its obligations to perform under this Contract, except with the prior written consent from APTS/Department.

I.24. Subcontracts

The Vendor shall notify the APTS/Department in writing of all subcontracts awarded under this contract if not already specified in the bidder's proposal. Such notification, in the original bid or later, shall not relieve the Vendor from any liability or obligation under the contract. Subcontract shall be only for bought-out items and sub-assemblies.

I.25. Delays in the supplier's performance

1. Delivery of the Goods and performance of the services shall be made by the Vendor in accordance with the time schedule specified by the APTS/Department in the specifications.
2. If at any time during performance of the Contract, the Vendor should encounter conditions impending timely delivery of the goods and performance of services, the Vendor shall promptly notify the APTS/Department in writing of the fact of the delay, its likely duration and its cause(s). As soon as practicable after receipt of the vendor's notice, APTS/Department shall evaluate the situation and may at its discretion extend the Vendor's time for performance, with or without liquidated damages.
3. A delay by the Vendor in the performance of its delivery obligations shall render the vendor liable to the imposition of appropriate liquidated damages, unless an extension of time is agreed upon by APTS/Department without liquidated damages.

I.26. Liquidated damages

If the Vendor fails to deliver any or all of the goods or perform the services within the time period(s) specified in the Contract, the APTS/Department shall, without prejudice to its other remedies under the Contract, deduct from the Contract Price, as liquidated damages, a sum equivalent to, as per the terms indicated in the bid document, until actual delivery or performance, subject to maximum limit. Once the maximum is reached, the APTS/Department may consider termination of the contract.

I.27. Termination for default

1. The APTS/Department, without prejudice to any other remedy for breach of Contract, by written notice of default sent to the Vendor, may terminate the Contract in whole or in part:
    a. if the Vendor fails to deliver any or all of the Goods/services within the time period(s) specified in the contract, or within any extension thereof granted by the APTS/Department pursuant to Clause 25 of GCC or
    b. if the Vendor fails to perform any other obligation(s) under the Contract or
    c. if the Vendor, in the judgment of the APTS has engaged in corrupt or fraudulent practices in competing for or in executing the Contract.
2. In the event the APTS/Department terminated the contract in whole or in part, APTS/Department may procure, upon such terms and in such manner as it deems appropriate, goods or services similar to those undelivered, and the Vendor shall be liable to the APTS/Department for any excess costs for such similar goods or services. However, the Vendor shall continue performance of the contract to the extent not terminated.

I.28. Force majeure

1. The Vendor shall not be liable for forfeiture of its performance security, liquidated damages, or termination for default if and to the extent that its delay in performance or other failure to perform its obligations under the Contract is the result of an event of Force Majeure.
2. For purposes of this clause, “Force Majeure” means an event beyond the control of the Vendor and not involving the Supplier’s fault or negligence and not foreseeable. Such events may include, but are not restricted to, acts of the APTS/Department in its sovereign capacity, wars or revolutions, fires, floods, epidemics, quarantine restrictions and freight embargoes.
3. If a Force Majeure situation arises, the Vendor shall promptly notify the APTS/Department in writing of such condition and the cause thereof. Unless otherwise directed by the APTS/Department in writing, the Vendor shall continue to perform its obligations under the Contract as far as is reasonably practical, and shall seek all reasonable alternative means for performance not prevented by the Force Majeure event.

I.29. Termination for insolvency

APTS/Department, may at any time terminate the contract by giving 30 days written notice to the Vendor if the Vendor becomes bankrupt or otherwise insolvent. In this event, termination will be without compensation to the Vendor, provided that such termination will not prejudice or affect any right of action or remedy which has accrued or will accrue thereafter to the APTS/Department.

I.30. Termination for convenience

1. APTS/Department, may at any time by giving 30 days written notice to the Vendor, terminate the Contract, in whole or in part, for its convenience. The notice of termination shall specify that termination is for the APTS/Purchaser's convenience, the extent to which performance of the Vendor under the Contract is terminated, and the date upon which such termination becomes effective.
2. The goods that are complete and ready for shipment within thirty (30) days after the vendor's receipt of notice of termination shall be accepted by the APTS/Department at the contract terms and prices. For the remaining Goods, the APTS/Department may elect to have any portion completed and delivered at the contract terms and prices at its discretion.

I.31. Resolution of disputes

1. APTS/Department and Vendor shall make every effort to resolve amicably by direct informal negotiation any disagreement or dispute arising between them under or in connection with the contract.
2. If, after thirty (30) days from the commencement of such informal negotiations, the APTS/Department and the Vendor have been unable to resolve amicably a contract dispute, either party may require that the dispute be referred for resolution to the formal mechanisms specified here in. These mechanisms may include, but are not restricted to, conciliation mediated by a third party.
3. The dispute resolution mechanism shall be as follows:
4. In case of a dispute or difference arising between the APTS/Department and the Vendor relating to any matter arising out of or connected with this agreement, such disputes or difference shall be settled in accordance with the Arbitration and Conciliation Act, of India, 1996.

I.32. Governing language

The contract shall be written in English or Telugu. All correspondence and other documents pertaining to the contract which are exchanged by the parties shall be written in same languages.

I.33. Applicable law

The contract shall be interpreted in accordance with appropriate Indian laws.

I.34. Notices

1. Any notice given by one party to the other pursuant to this contract shall be sent to the other party in writing or by telex, email, cable or facsimile and confirmed in writing to the other party's address.
2. A notice shall be effective when delivered or tendered to other party whichever is earlier.

I.35. Taxes and duties

The vendor shall be entirely responsible for all taxes, duties, license fee Octroi, road permits etc. incurred until delivery of the contracted Goods/services at the site of the user or as per the terms of tender document if specifically mentioned. However any new taxes introduced by GoI / GoAP during validity of the contract it will be applicable to both parties (i.e. Supplier / Purchaser)

I.36. Licensing considerations

The software mentioned in the Schedules of Requirement will be used throughout Andhra Pradesh or user's sites even outside Andhra Pradesh.

I.37. Protection against damages- site conditions:

1. The system shall not be prone to damage during power failures and trip outs. The normal voltage and frequency conditions available at site are as under:
    a. Voltage 230 Volts
    b. Frequency 50Hz.
2. However, locations may suffer from low voltage conditions with voltage dropping to as low as 160 volts and high voltage conditions with voltage going as high as 220 + 20% volts. Frequency could drop to 50Hz + 2%. The ambient temperature may vary from 10oC to 48oC. The relative humidity may range in between 5% to 95%.
3. The goods supplied under the contract should provide protection against damage under above conditions.

I.38. Fail-safe procedure

The vendor should indicate in detail fail-safe procedure(s) for the following:

1. Power failure
2. Voltage variation
3. Frequency variation
4. Temperature and humidity variations.

I.39. Training:

For each hardware and software component installed, for the devices, the Vendor may be required to train the designated APTS and user personnel to enable them to effectively operate the total system. The training, if required, shall be given, as specified in the SCC at the locations specified. The training schedule will be agreed to by both parties during the performance of the Contract.

I.40. Site Preparation and Installation:

The Purchaser is solely responsible for the construction of the installation sites except where it is specifically required under bid document. The bidder will designate to perform a site inspection to verify the appropriateness of the sites before the installation of every hardware related item.

I.41. Delivery Terms & Conditions:

a) Physical Inspection and preliminary testing of the products shall be done at TRANSPORT COMMISSIONER Head Office in the presence of representatives of the vendor and will comprise of the following.

i. Physical verification of equipment as per the supply contract.
ii. Physical inspection of the equipment for any physical damage.
iii. "Power on Self-test" to ascertain that no product is dead on arrival.
iv. Physical verification of licenses, software media, technical documentation as per purchase order.
v. Registering the Hardware & software license with OEM for validation and desired technical support.
vi. Should the inspected or tested components fail to confirm to the contract, the TRANSPORT COMMISSIONER may reject the components, and the Vendor shall with in permitted delivery period, replace the rejected components, so that it meets the Contract requirements free of cost.

b) After Physical verification, Vendor should deploy the firewalls to the Branch Offices of TRANSPORT COMMISSIONER for Physical installation, configuration as per the requirement at free of cost.

I.42. Disaster Recovery Site:

Vendor should be able to extend the solution to the DR site whenever the need arises.

I.43. Security features:

Should ensure secure on-boarding of users to Network Firewall from trusted as well as untrusted network.

I.44. Availability:

The solution should be configured in high availability mode and should ensure there is no single point of failure. Availability of the solution should be 99.9% uptime to be analyzed on quarterly basis.

Section J – Special Conditions of Proposed Contract (SCC)

Section K – Model Contract Form

Contract Ref No: _____

THIS AGREEMENT is made on ____ day of _____

BETWEEN

1. *The Managing Director , Andhra Pradesh Technology Services Limited*, APTS Ltd, 3rd Floor, R&B Building, MG Road, Labbipet,Vijayawada-500010, Andhra Pradesh, India or HoD of User Department (hereinafter called "the Purchaser"),on behalf of _____ Department, AP and

2. _____a company incorporated under the laws of India and having its registered office at _____. (Hereinafter called "the Supplier").

WHEREAS the Purchaser invited bid for certain goods and ancillary services viz., *Supply and Installation of* _____ *for supply at* _____ and has accepted a bid by the Supplier for the supply of those goods and services in the sum of Rs. _____ (_____.) including all taxes and duties (hereinafter called as "the Contract Price")

NOW THIS AGREEMENT WITNESSETH AS FOLLOWS:

In this Agreement words and expression shall have the same meanings as are respectively assigned to them in the Conditions of bid document referred to

1. Scope of the Work

   Brief outline of the work: To *Supply & Installation of devices/products/items as per the staggered orders issued time to time during the contract period* _____*at* _____. The detailed scope is as covered in RFP and subsequent clarifications.

2. Contract Documents

   2.1. Contract Documents

   The following documents shall constitute the Contract between the User and the Supplier, and each shall be read and construed as on integral part of the Contract:

   I. This Contract Agreement and the Annexures attached to the Contract Agreement
   II. Notification of award
   III. Minutes of TCPC meeting held on _____
   IV. Pre – bid conference minutes
   V. Bid document Ref No. _____Dt. _____

2.2. Order of Precedence

In the event of any ambiguity or conflict between the Contract Documents listed above, the order of precedence shall be the order in which the Contract Documents are listed in 2.1(Contract Documents) above, provided that Schedule of Amendments contained in Annexure IV shall prevail over all provisions of the Contract Agreement and the other Appendices attached to the Contract Agreement and all the other Contract Documents listed in 2.1 above.

3. In consideration of the payments to be made by the Purchaser to the Supplier as hereinafter mentioned, the Supplier hereby covenants with the Purchaser to provide the Goods and Services and to remedy defects therein in conformity in all respects with the provisions of the Contract.

4. The Purchaser hereby covenants to pay the Supplier in consideration of the provision of the Goods and Services and the remedying of defects therein, the Contract Price or such other sum as may become payable under the provisions of the Contract at the times and in the manner prescribed by the Contract.

5.1. Brief particulars of the goods and services which shall be supplied /provided by the supplier are as under:

Sl. No	Solution, service, or material	Max. Qty	Unit Price
1.			
2.			
3.			
	Grand Total		

5.2 DELIVERY SCHEDULE :_____
5.3 WARRANTY: :_____
5.4 SUPPLIERS RESPONSIBILITY :_____
5.5 UP TIME % : :_____
5.6 EXIT CLAUSE : :_____
5.7 PAYMENT TERMS :_____

IN WITNESS WHEREOF the Purchaser and the Supplier have caused this Agreement to be duly executed by their duly authorized representatives the day and year first above written.

For and on behalf of the Purchaser

Signed:_

In the capacity of Managing *Director, APTS / HoD of User Department*

in the presence of _____

For and on behalf of the Supplier

Signed:_

in the capacity of----------, *M/s.* _____

in the presence of _____

Items	Configuration Required	Qty	Unit Price

Annexure – IV

Amendments & Other Documents

S.No.	Amendment No	Date	Amendment Description

Section L – Annexures

Annexure I – Bid Security (EMD) BG Form

APTS Ref. No.....

Bid Security (EMD) Form

(To be issued by a bank scheduled in India and having at least one branch in Vijayawada)

Whereas..... (Here in after called "the Bidder") has submitted its bid Dated ……..... (Date) for the execution of..... (Here in after called "the Bid")

KNOW ALL MEN by these presents that We ..... of ..... having our registered office at..... (hereinafter called the "Bank") are bound into the Andhra Pradesh Technology Service Ltd. (hereinafter called "The APTS") in the sum of ..... for which payment well and truly to be made to the said APTS itself, its successors and assignees by these presents.

The conditions of this obligation are:

1. If the bidder withdraws its bid during the period of bid validity or
2. If the bidder, having been notified of the acceptance of its bid by the APTS during the period of bid validity:
    a. fails or refuses to execute the contract form if required; or
    b. fails or refuses to furnish the performance security, in accordance with the bid requirement;
    c. Submits fake documents.

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

This guarantee will remain in force up to and including 45 days after the period of the bid validity, and any demand in respect thereof should reach the Bank not later than the above date.

Place:
Date:

Signature of the Bank
and seal.

Annexure II – Performance Security BG Form

APTS Ref. No.....

Performance Security Form

(To be issued by a bank scheduled in India and having at least one branch in Vijayawada)

To: ..... (Address of APTS/HOD)

WHEREAS..... (Name of Vendor) hereinafter called "the Vendor" has undertaken, in pursuance of Contract No..... Dated ... (Date), to supply..... called "the Contract".

AND WHEREAS it has been stipulated by you in the said Contract that the Vendor shall furnish you with a Bank Guarantee by a recognized bank for the sum specified therein as security for compliance with the Supplier's performance obligations in accordance with the Contract.

WHEREAS we have agreed to give the Vendor a Guarantee:

THEREFORE, WE hereby affirm that we are Guarantors and responsible to you, on behalf of the Vendor, up to a total of Rs. ..... and we undertake to pay you, upon your first written demand declaring the Vendor to be in default under the Contract and without cavil or argument, any sum or sums within the limit of Rs..... . (Amount of Guarantee) as aforesaid, without your needing to prove or to show grounds or reasons for your demand or the sum specified therein.

This guarantee is valid until the ..... day of..... (Date)

Place:

Date: Signature and seal of guarantors

Annexure III – Manufacturer's Authorization Form

APTS Tender ref.no.

Manufacturer Authorization

The authorization should be in the nature of a letter, memorandum or certificate regularly granted by the manufacturer to its channel partners, authorized solution providers, system integrators, distributors, etc. or a specific letter issued for purposes of this bid. Such communication should include statements / undertakings from the said manufacturer to the following effect:

1. Guarantee and warranty coverage in respect of the goods and services manufactured by the said manufacturer shall be honored by that manufacturer, their channel partners, distributors, authorized service centers as the case may be.
2. The manufacturer updates the bidder and their technical personnel with relevant technical literature, training and skill transfer workshops etc. on a regular basis.
3. The manufacturer provides back-to-back technical support to the said bidder on a continuing basis.
4. The said bidder is authorized to provide service and solutions using hardware, firmware and software as the case may be.

Note:
The letter of authority should be signed by a person competent and having the power of attorney to bind the manufacturer.

Annexure IV – Model Installation cum AT Report

(On Company Letterhead with other statutory details)

IR No., IR date

Office Name & Location:

I. Desktop/AIO/Laptop Make/Model: Qty:

S.NO. : (Attach separate sheet quantity is more)

SN	Complete specifications as per RFP/Tender Document are to be mentioned such as	Functionality
1	Processor Details	
2	Chipset Details	
3	Memory: RAM	
4	Hard Disk: Make, Model & Capacity	
5	Monitor Details	
6	DVDRW	
7	Network Adapter(s)	
8	Wireless	
9	Integrated / External Speakers (Make)	
10	Ports	
11	Graphics	
12	Key board & Mouse	
13	Antivirus	
14	Operating System	
15	Warranty Period	
16	**Installation observations**	Working satisfactorily or observations found if any

II. Printers : Qty: S.No:

SN	Complete specifications as per RFP/Tender Document are to be mentioned such as	Functionality
1	Make, Model	
2	Printing Technology	

3	Printer Functions: Print/Scan/Copy/FAX/Color/Mono etc.	
4	Memory	
5	Printing Speed	
6	Details of Toner Cartridge supplied	
7	Cables & Driver CDs supplied	
8	Warranty Period	
9	**Installation observations**	Working satisfactorily or observations found if any

III. Scanners : Qty: S.No:

SN	**Complete specifications as per RFP/Tender Document are to be mentioned**	**Functionality**
1	Make, Model	
2	Scanner type such as Flatbed/Flatbed with ADF/RADF etc.	
3	Speed	
4	Resolution	
5	Cables & Driver CDs supplied	
6	Warranty Period	
7	**Installation observations**	Working satisfactorily or observations found if any

IV. UPS: Qty: S.No:

SN	**Complete specifications as per RFP/Tender Document are to be mentioned**	**Functionality**
1	Make, Model	
2	Capacity & Technology	
3	Input/ Output Voltages observed	
4	Power Factor	
5	AC-AC efficiency	
6	Batteries Make & Model	
7	Battery Capacity & Nos.	
8	Battery Rack Supplied (Y/N)	
9	All required cables supplied (Y/N)	
10	Warranty Period	
11	**Installation observations**	Working satisfactorily or observations found if any

V. Any Other Components:

SN	Complete specifications as per RFP/Tender Document are to be mentioned	Functionality
1		
2		
3		
4		
5	Warranty Period	
6	**Installation observations**	Working satisfactorily or observations found if any

General Remarks:

Signature of Installation Engineer
Name
Contact No.

Signature of Dept. Official
with Name, Contact No., Seal & Date

Section M – Bid Forms

Bid Letter Form

From:
(Registered name and address of the bidder.)

To:
Andhra Pradesh Technology Services Ltd,
3rd Floor, R&B Building, MG Road, Labbipet,
Vijayawada-520010, Andhra Pradesh, India

Sir,

Having examined the bidding documents and amendments there on, we the undersigned, offer to provide services/execute the works including supply, delivery installation of hardware, firm wares and softwares as the case may be, in conformity with the terms and conditions of the bidding document and amendments there on, for the following project in response to your tender Ref. no _____call dated .....

Project title:

We undertake to provide services/execute the above project or its part assigned to us in conformity with the said bidding documents in accordance with the schedule of prices attached herewith/submitted through online bid and coverage options made by APTS or its user organization.

If our bid is accepted, we undertake to;

1. Provide services/execute the work according to the time schedule specified in the bid document,
2. Obtain the performance guarantee of a bank in accordance with bid requirements for the due performance of the contract, and
3. Agree to abide by the bid conditions, including pre-bid meeting minutes if any, which remain binding upon us during the entire bid validity period and bid may be accepted any time before the expiration of that period.

We understand that you are not bound to accept the lowest or any bid you may receive, nor to give any reason for the rejection of any bid and that you will not defray any expenses incurred by us in bidding.

Place:
Date:

Bidder's signature
and seal.

Form P-1 - Bidder Information

1	Name of the organization	
2	Year of establishment	
3	Registered Office Address	
4	Phone No.	
5	Fax No.	
6	Email	
7	Contact person details with phone no.	
8	Total No. of branch offices in AP	
9	Total Support engineers at -	
10	At Head office (No.)	
11	At branch offices (No.)	
12	Whether Manufacturer?	If Yes, Provide relevant documents
13	Whether authorized dealer/ Service Provider?	If Yes, Provide relevant documents
14	Details of EMD furnished	
15	Details of certificates enclosed.	
16	Details of Purchasing document.	Provide details like APTS Receipt No& Date.

Place:
Date:

Bidder's signature
and seal.

Form P-2 – Bidder Turnover Details

Turnover details as per pre-qualification criteria mentioned in Section B of this document (taking in to consideration all the amendments issued to this document if any) are to be provided along with supporting documents.

Turnover Details

Sl. No.	Financial Year	Turnover of the bidder in Rs.	Profit after Tax (Rs.)	Networth in Rs.
	(1)	(2)	(3)	(4)
1				
2				
3				

Place:
Date:

Bidder's signature and seal.

Form P-3 - List of Major Customers

S.No	Customer Full Address	Year of supply	Items supplied to the customer
A	B	C	D

Form P-4 - Details of service centers in AP

S.No	Full Address of service center	Contact person with phone No.	No. of support engineers
A	B	C	D

Form P-5 - Declaration Regarding Clean Track Record

To,
The Managing Director
Andhra Pradesh Technology Services Limited
3rd Floor, R&B Building, MG Road, Labbipet,
Vijayawada-520010, Andhra Pradesh, India

Sir,

I have carefully gone through the Terms & Conditions contained in the RFP Document [No._____]. I hereby declare that my Company/Consortium Partners has not been debarred/ black listed as on Bid calling date by any State Government, Central Government, Central & State Govt. Undertakings/enterprises/Organizations and by any other Quasi Government bodies/Organizations, in India for non-satisfactory past performance, corrupt, fraudulent or any other unethical business practices. I further certify that I am competent officer in my company to make this declaration.

Yours faithfully,

(Signature of the Bidder)
Printed Name
Designation
Seal
Date:
Business Address:

Form P6 – Undertaking in compliance with GFR Rule 144(xi)

Ref: Date:

To
The Managing Director,
AP Technology Services Ltd, 3rd Floor, R&B Building
M.G. Road, Vijayawada – 520010

Dear Sir,

Sub: Tender for Selection of Service Provider for Supply and Installation of Network Firewall and Technical Support for Transport Department Offices across AP.– Regarding.

Ref: Tender Reference _____

I/We, < Bidder / OEM Name> have read the clause regarding restrictions on procurement from a Bidder/ OEM of a Country which shares a land border with India.

I/We hereby certify that I/We, <OEM/Bidder Name> is not from any such country or, if from such a Country, has been registered with the following Competent Authority:

1. Details of competent authority:
2. Registration Certificate Ref. No.: (copy to be enclosed)
3. Products for which registered: (registration should be valid for the offered product)

I/We hereby certify that I/We in the event of becoming a successful bidder shall not sub-contract works to any Contractor from a Country which shares a land border with India unless such Contractor is registered with the Competent Authority, as per GFR rule 144(xi).

I/We hereby certify that I/We fulfill all requirements in this regard and eligible to be considered

For <OEM/Bidder>

Authorized signatory:
Name of the authorized person:
Designation:
Name of Bidder: Stamp of Bidder:

NOTE:

1. The letter should be submitted on the Letter head of the Bidder / OEM and should be signed by the Authorized signatory.
2. Any deviation would lead to summary rejection of bids.
3. Where Applicable, evidence of valid registration of the Competent Authority shall be attached.

Form T 1 – Technical Compliance Statement

Item wise technical compliance statement as per technical specifications mentioned in Section-D of this document (taking in to consideration all the amendments issued to this document, if any) is to be submitted in the following format:

Item Code:
Item Name:

Sl. No.	**Parameter/ Feature**	**Specification Required**	**Specification of proposed item along with Part Code, Qty. & Description if any (Part code details must be provided if available)**	**Compliance (Complied/Higher/Lower)**	**Reference for proof of compliance** **(Required docs to be uploaded along with technical bid)**
A	B	C	D	E	F
					(Detailed reference such as doc name, para no. page no. etc. should be provided)

Form T 2 - Checklist

Compliance/Agreed/Enclosed/ Deviation Statement

The following are the particulars of compliance/deviations from the requirements of the tender specifications.

Sl.No.	Bid document reference	Remarks
1.	Delivery period	
2.	Bid letter Form	
3.	Form P-1	
4.	Form P-2	
5.	Form P-3	
6.	Form P-4	
7.	Form P-5	
8.	Form P-6	
9.	Manufacturer's Authorization Form	
10.	Form T-1	
11.	Form T-2	
12.	Form T-3	
13.	Form F-1 (unpriced)	
14.	Pre-qualification criteria	
15.	Technical specifications	
16.	General instruction to bidders	
17.	Standard procedure for bid evaluation	
18.	General condition of proposed Contract (GCC)	
19.	Special Condition of proposed Contract (SCC)	

The specifications and conditions furnished in the bidding document shall prevail over those of any other document forming a part of our bid, except only to the extent of deviations furnished in this statement.

Place: Bidder's signature
Date: and seal

NOTE:
For every item appropriate remarks should be indicated like 'no deviation', 'agreed', 'enclosed' etc. as the case may be.

Form T3 – Model declaration form for undertaking of authenticity for IT Hardware Supplies

Undertaking of authenticity for IT Hardware Supplies

1. This has reference to IT Hardware to be supplied/quoted in case we selected for the RFP Ref. No. _____ dated _____

2. We hereby undertake that all the components/parts/assembly/software used in the IT Hardware Supplies like Hard disk, Monitors, Memory etc shall be original new components/parts/ assembly/software from respective OEMs of the products and that no refurbished/duplicate/second hand components/parts assembly/software are being used or shall be used.

3. We undertake that the supplied equipment will be 100% in accordance with the specifications and features mentioned in the RFP/Tender.
    a. We will prepare to the annexure to installation report and will be given to installation/service engineers while going for installation of equipment or devices.
    b. Our Service Engineer/Installation engineer will demonstrate all the features and functions to the end user during the installation and obtain the signature installation report and annexure to the installation report.

4. We also undertake that in respect of licensed operating system if asked by you in the purchase order shall be supplied along with the authorized license certificate (eg Product Keys on Certification of Authenticity in case of Microsoft Windows Operating System) and also that it shall be sourced from the authorized source (eg Authorized Microsoft Channel in case of Microsoft Operating System)

5. Should you require, we shall produce certificate from our OEM Supplier in support of above undertaking at the time of delivery. It will be our responsibility to produce such letters from our OEM supplier's within a reasonable time.

6. In case we are found not complying with above at the time of delivery or during installation, for the IT Hardware already billed, we agree to take back such items if already supplied and return the money if any paid to us by you in this regard.

Authorized Signatory

Name

Designation

Cost Sheets - Form F1

Sl. No.	Item details with make and model	Unit Price without taxes (Rs.)	Taxes/ Duties etc on unit Price (Rs.)	Unit Price with all taxes (Rs.)	QTY (Nos.)	Total price with taxes and duties etc (Rs.)
1	**2**	**3**	**4**	**5**	**6**	**7**
1	Item 1: Firewall Appliance: Hardware and Software subscription with 24x 7 online support and Implementation with 5 years warranty with support.				**67**	
2	Item 2: Firewall Appliance: Hardware and Software subscription with 24x 7 online support and Implementation with 5 years warranty with support.				**31**	
3	Item 3: Firewall Appliance: Hardware and Software subscription with 24x 7 online support and Implementation with 5 years warranty with support.				**01**	
Total Price (Inclusive of all Taxes) (Rs.)						

(Signature of Bidder)

Note:-

1. Evaluation of Financial Bids will be including taxes.
2. L1 will be decided on the Total Cost. Least Value Bid in the reverse auction shall be considered as successful bidder.