# भारतीय प्रौद्योगिकी संस्थान पटना

# INDIAN INSTITUTE OF TECHNOLOGY PATNA

बिहटा, पटना–801106, बिहार, भारत

**Bihta, Patna – 801 106, Bihar, INDIA**

## E-PROCUREMENT MODE

**Invitation of Expression of Interest**

**For**

**Study, Upgradation, Configuration, Testing, Commissioning of Next Generation Firewall Solutions with 05 Years Warranty at IIT Patna**

**Estimated Budget: INR 1.00 Cr.**

भारतीय प्रौद्योगिकी संस्थान पटना
INDIAN INSTITUTE OF TECHNOLOGY PATNA
बिहटा, पटना–801106, बिहार, भारत
Bihta, Patna – 801 106, Bihar, INDIA

**EoI Reference No.: IITP/S&P/EPR/1/CC-89/2022-23** **Date: 20.09.2022**

Indian Institute of Technology Patna is in the process of extending Data and Telephone Connectivity to upcoming sites in campus as per the details as given as under:

| | |
|---|---|
| **Name of Expression of Interest (EoI)** | Study, Upgradation, Configuration, Testing, Commissioning of Next Generation Firewall Solutions with 05 Years Warranty at IIT Patna |

1. Detailed Tender/EoI Documents may be downloaded from Central Public Procurement Portal (https://eprocure.gov.in/eprocure/app) and from our website (https://www.iitp.ac.in/).
2. All details /document pertaining to the tender/EoI such as tender/EoI document, pre-bid report, corrigendum and any further updates will be available only on our website & also at CPP Portal.
3. **No manual bid/EoI will be accepted. All quotations/proposals (both technical & financial) should be submitted in the e-procurement portal only.**
4. IIT Patna shall not be responsible for non-receipt of bid due to internet issues or any other reasons.

## CRITICAL DATES

| | |
|---|---|
| Date of Issue/Publication of EoI | 21.09.2022 (03:00 PM) |
| EoI Document Download Start Date | 21.09.2022 (03:00 PM) |
| EoI Submission Start Date | 21.09.2022 (03:00 PM) |
| Last Date and Time for submitting e-mail queries regarding technical specifications and other conditions of EoI document | 06.10.2022 (03:00 PM) |
| Pre-bid meeting | 11.10.2022 (11:00 AM) |
| EoI Document Download End Date | 25.10.2022 (03:00 PM) |
| Last Date and Time for uploading of response to EoI | 25.10.2022 (03:00 PM) |
| Opening Date and Time of Bid Online | 26.10.2022 (03:30 PM) |
| Physical / Online presentation Date & Time. The prospective bidders desirous to bid may attend the physical meeting or alternatively join the meeting with the following link : …… | Will be communicated to bidders later after submission of response to EoI. |
| Tentative Schedule for Floating RFP/Tender | 09.11.2022 (03:00 PM) |
| Address of Communication | The Registrar (for Stores & Purchase),<br>Indian Institute of Technology Patna<br>Kanpa Road, Bihta, Patna, Bihar-801106<br>Phone: 06115-233-683 |
| For taking technical assistance regarding bid submission, if any | CPP Portal Website: https://eprocure.gov.in<br>Help Desk Number 0120-4200462, 4001002, 4001005 and 4001005. |

**REGISTRAR, IIT PATNA**

## Table of Contents

# 1. Introduction

The campus data and telephone network at IIT PATNA provides the high performance, resilient, highly available and scalable LAN, Internet and IP telephone service to the students and employees working and residing at the campus. It comprises both wired and wireless networks spanning across academic, hostels and residential areas. There are approximately 850 IP phones, 5000 information outlets (IO) and 100 wifi access points in the LAN and approximately 22 Km single mode OFC (48 core) is laid down across the campus in ring-star topology. This hybrid network is capable of providing data and voice service through 10-gigabit optical backbone along with wireless connectivity through indoor access points.

There are adequate redundancies present in the critical resources located at the core and distribution layer of the network for service continuation in case of faults. For ease of operations, the entire campus is divided into five zones:

- The admin and academic zone- Admin blocks, academic blocks and tutorial blocks
- The Hostel zone- Girl's and Boy's Hostels
- The Residential zone- A,B,C,D type quarters, Director Bunglow, Guest house
- The Campus services zone- School, Hospital, CPWD office, IC etc.
- The Core zone- Block 9 network server where core components are hosted

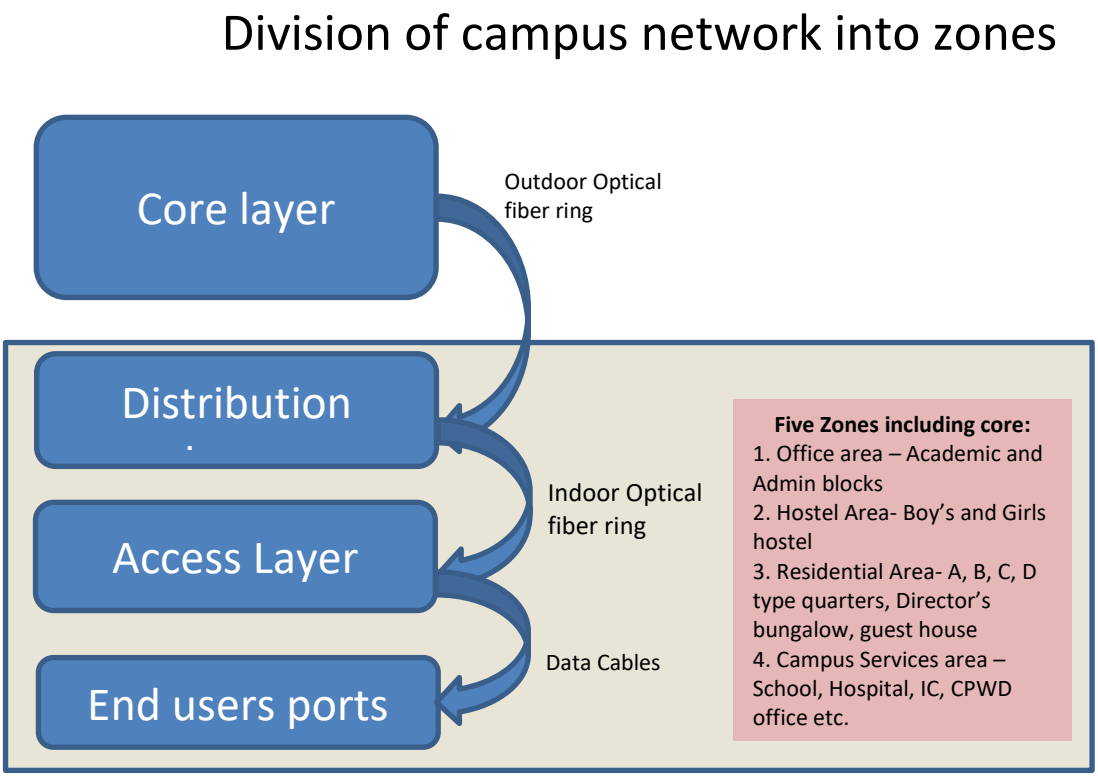


Figure 1: Three layer design with network zones

| | |
|---|---|
| **Existing Firewall** | CSCO ASA 5585-X SSP-20, FirePOWER SSP-20,16GE,4GEMgt,1AC,3DES/AES |
| **Number of ISPs** | 2 to 3 |
| **Bandwidth of ISPs** | Currently 1 Gbps, may be upgraded to 10 Gbps |
| **ISP to Firewall Connectivity** | Copper/Fiber |
| **ISP Load Balancing Requirement** | Yes |
| **Number of Users** | 5000-7000 |
| **Number of Concurrent users** | 2000 |
| **Internal campus hosted servers to be published to internet via firewall** | Web Server/Mail Server/SFTP Server/ |
| **LAN Infrastructure -some numbers** | Core Switch-2,<br>Distribution Switches- Currently 15 but it will grow to 50,<br>access-200+ expected to grow further<br>Wifi APs-150+ |
| **How many intranet/LAN interfaces ? Specify the type of interface (Copper/Fibre/10 Gig Fibre)** | 8 X 1G , 8X10G from day 1<br>Provision to expand to 2X40G |
| **Number of campus/Branch** | 1 |
| **VPN** | SSL/IPSEC |
| **Concurrent VPN users** | 500 |
| **Sandboxing- For Zero day threat prevention** | yes |

# 2. Invitation for Expression Of interest

## Objective

Overall objective of this EoI is to invite Agencies with proven capabilities for "Study, Upgradation, Configuration, Testing, Commissioning with 05 Years Operations, Support and Maintenance of Next Generation Firewall Solutions".

From cyber and digital security perspective, the campus network can be visualized with following domains:

- **User Domain:** Actual users.
- **Workstation Domain:** Workstations and printers.
- **Wireless Domain:** Wifi APs and its interfacing with Wifi enabled devices like laptops, mobiles etc.
- **LAN Domain:** Physical and logical LAN technologies (100Mbps/1000Mbps switched Ethernet) used to support workstation connectivity to the organization's network infrastructure.
- **LAN-to-WAN Domain:** Routers, firewalls, demilitarized zones (DMZs), and IDS/IPS.
- **WAN Domain:** Routers, circuits, switches, firewalls, gateways, and equivalent gear at remote locations, mostly under a managed service offering by the service provider.
- **Remote Access Domain:** Virtual private networks (VPNs), laptops with VPN software, and secured socket layer/VPN (SSL/VPN) tunnels.
- **System/Application Domain:** Servers, campus hosted softwares and services, like Database, Websites, DNS, Directory services, client/server applications, and data typically housed in a data center or server rooms.

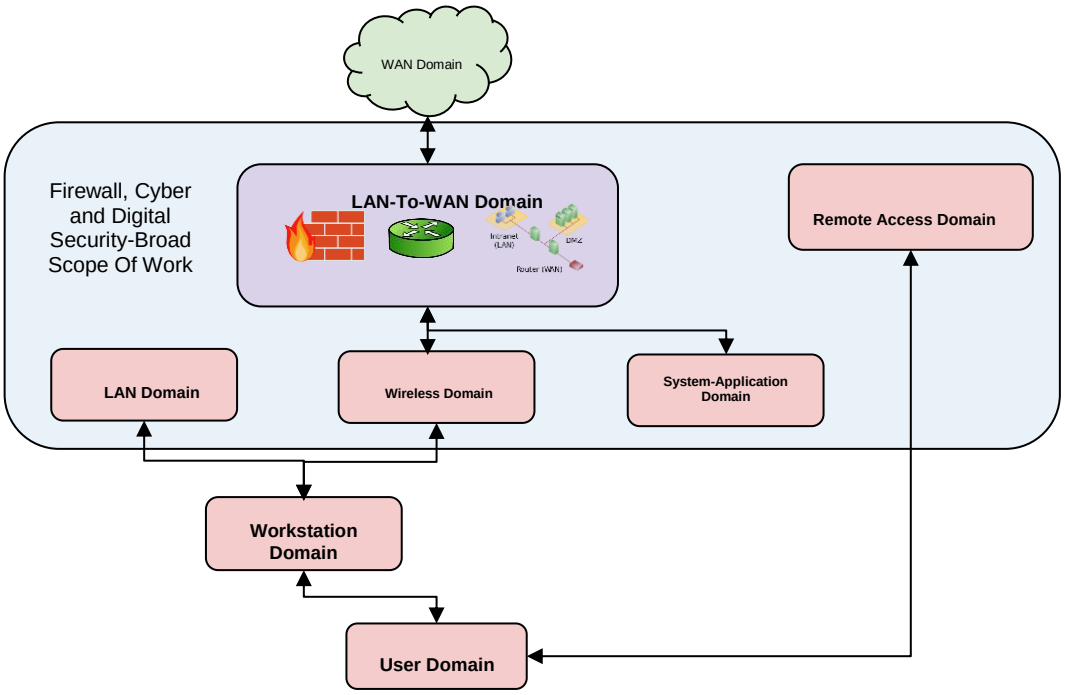


Figure 2: Different logical domains from cyber and digital security perspective

Through this EoI, capable bidders/OEM are invited for providing the solution to strengthen the domains highlighted in figure

## Selection Procedure

Each bidder shall participate in the following stages:

Stage I: Pre-Qualification based selection of bidders.

Stage II: Technical Presentation of Solution.

Stage III: Floating RFP/Tender to the bidders selected through Stage I and selection of final bidder through technical and financial evaluation as per RFP/Tender.

Each shortlisted bidder based on the pre-qualification criteria shall mandatorily participate in Technical Presentation of the Solution which forms an integral part of the EoI process. Final selection shall be done based on response to the RFP/Tender floated to qualifying bidders in this EoI and shall include the financial bid. It is important to note that only selected vendors through this EoI shall be eligible to participate in the RFP/Tender stage. The section 5 describes the broad scope of work that shall be carried out by the bidder who is selected in the RFP/Tender stage.

**Some salient terms and conditions about this EoI:**

| | |
|---|---|
| 1 | The Expression of Interest must be accompanied with duly filled Information sheets and sufficient documentary evidence. Expression of Interest with incomplete Information or insufficient documentary evidence shall be rejected. |
| 2 | IIT PATNA reserves the right to modify, expand, restrict, scrap, and refloat the Expression of Interest. |
| 3 | Formal Tender/Bid(Technical and Financial bids) will be invited later from the eligible/qualifying firms based on the EOI submitted and presentation. Physical presence of the firms shall be mandatory at the time of presentation of solution in response to the EOI submitted before to the committee. No EOI shall be considered in absence of detailed technical presentation of the complete solution on the dates decided by the Institute. |
| 4 | Clarification: Clarification, if any, about the requirement can be obtained by visiting the Computer Centre with prior information. |
| 5 | It will be the sole discretion of IIT PATNA to or not to incorporate any changes in the requirement based on feedback/input/suggestions received during the presentation/discussion. The decision of the IIT PATNA regarding acceptability of any suggestion shall be final in this regard. |
| 6 | Only shortlisted bidders/vendors who have participated in the EOI will be allowed to finally submit their quotation (technical and financial). Those who have not been shortlisted in EOI will not be allowed to submit their quotation and the quotation received from any such vendor will be rejected. Hence all the prospective bidders are requested to participate in EOI. |
| 7 | The bidder (OEM/ System Integrator) is required to do the site survey and submit the complete solution with EOI including design, drawing. |
| 8 | The survey shall be carried out by nominated authorized person/team by the bidder with prior permission of the institute authorities. This includes cabling plan, network structure plan, network design and complete solution. |

# 3. On-site Presentations

The participating applicants shall be called for on-site presentations after the proposal due date (tentatively within two weeks of proposal due date). The schedule of such presentations will be communicated to the participating applicants through mail.

# 4. Pre-Qualification/Essential Eligibility Criteria

| Sl. No. | Technical | Compliance (Y/N) | Page No. in Bid Doc. & Packet no. |
|---|---|---|---|
| 1 | Valid ISO and CMMI certification - ISO/IEC 20000-1 international standard for IT service management, ISO 9001:2000, ISO 9001:27000 and CMMI level 3. The relevant certification document with validity must be presented. | | |
| 2 | The bidders must have an office registered in India for at least five years. | | |
| 3 | The bidder should be in existence in India and providing IT Security services/ business (i.e. preferably in the area of implementation of Firewalls/ UTM/IPS) for a minimum of five year as on date of EoI. (Please submit proof, such as Registration Certificate etc for existence and purchase order/work order showing implementation since last three years.) | | |
| 4 | The vendor/bidder must be the Highest Level partner of the proposed OEM (Original Equipment Manufacturer). | | |
| 5 | The bidder should be able to provide services at PATNA, BIHAR. | | |
| 6 | The Bidder must have experience in executing at least two similar projects (value, user number, features) within the last 03 (Three) years. The bidder must produce the supporting documents Works order/purchase order and completion/performance certificates. | | |
| 7 | The bidder should be the one point contact for the entire project. | | |
| 8 | The products offered preferably have been implemented in at least 2 IIT, NIT, IISER, Institute of National Importance, Central Universities, Central Govt. PSUs. These installations should be live for at least for the last one year. | | |
| 9 | The product and features are certified from internationally or nationally recognised bodies like Internet Computer Security Association (ICSA) and should feature in leaders/top 5 products in relevant domains in internationally or nationally recognised rating bodies like Gartner or equivalent. | | |

| Sl. No. | Technical | Compliance (Y/N) | Page No. in Bid Doc. & Packet no. |
|---|---|---|---|
| 10 | Valid Manufacturer's Authorization Form (MAF) (Duly attested hard copy must be submitted with the bid documents.) bearing NIQ/Tender No. | | |
| 11 | The bidder should have a dedicated comprehensive support service center having minimum 02 OEM certified engineers for each product offered in this EoI. The engineers should have minimum 2 years working experience on the offered OEM or devices. | | |
| 12 | In addition to the above bidder should have resources capable of decommissioning the existing Firewall at IITP independently without support of existing OEM and commissioning the proposed solution smoothly so as to ensure there is no impact on Business Continuity for more than 01 day under any circumstances. Documents in support of the same must be submitted. | | |
| 13 | The Vendor/Bidder should not have been blacklisted by any Central/State Government Organization or PSU for any corrupt and fraudulent practice. An Undertaking by the Authorized Signatory on the letter head of the Vendor/Bidder should be submitted as a part of Technical Offer in format given at **Form-2**. | | |
| 14 | All the employees/operator deployed by the vendor for the digitization activity must comply with government's rules and regulations like Minimum Wages Act, Provident fund and ESI facility standard. | | |
| 15 | Bidder should be a well-established vendor registered (existing for minimum 5 years) as a company under Indian Companies Act. | | |
| 16 | For the financial and operational stability, the applicant should have an average annual turnover of the last three financial years of at least INR 10.00 (Ten) Crore. The CA certified financial statements must be provided along with **Form-3**. | | |
| 17 | The bidder must have registered net profit during the last 3 financial years. This should be an individual company's turnover and net profit and not that of a group of companies. Documents supporting Financial Statement (like Copies of published Annual Reports etc.) should also be supplied along with Technical offer. | | |

# 5. Broad Scope Of Work

In a bid to strengthen IT security of the IIT PATNA (IITP), Computer Center intends to upgrade the existing campus network security framework and Next Generation Enterprise Firewall having various security modules/ components deployed in High Availability mode (replacing the existing CISCO ASA firewall) at its network server room and creating DMZ in the network for internet facing applications. The objective of the exercise is the following:

- The broad scope of work as detailed in this section refers to the hardware, software/ licenses and services used for upgrading the campus network security and the Next Generation Firewall at the server room.
- The appliances must be implemented in HA Provision of all licenses/subscriptions like appliance, management Server, Operating System, Database (if required), up-gradation etc.
- Ensure Installation, implementation & maintenance of the Campus Network Security Framework and Firewalls as per IITP security architecture design & pattern of traffic.
- Comprehensive onsite warranty of 5 years for all the hardware/software under the project.
- Device rules / device policy definition and enforcement.
- Detect and block sophisticated attacks by enforcing security policies at various levels,prevent unauthorized access or malicious traffic within the IITP system or in the network, and ensure protection from zero day attacks and unknown threats.
- Enable IITP to ensure that all the IT assets are secure from threats for today, tomorrow and in the future.
- A detailed design has to be chalked out along with the project plan in the form of TAMD (Technical Approach and Methodology Document) detailing but not limited to the indicated points as mentioned in Annexure ____. The selected bidder shall be responsible for Design, Supply, Installation, Configuration, Testing and Commissioning of the solution at IITP.
- Generation and submission of necessary documents required during various phases of project viz. planning, installation, commissioning, rollout, acceptance testing, project diagrams and other reports etc. All such documents shall commence only after the same is approved by IITP.
- De-commissioning of existing Campus Firewall and related devices at IITP Server room i.e, replacing the existing firewall and related devices with the new campus network security framework and firewall in such a way that there is no impact on business continuity.
- Installation of the proposed appliance will include migration of policies and configuration of the existing Firewall device at IIT Server room.
- Installation, commissioning & configuration to be done in a single pass or in Phases, must be completed within 2 days under all circumstances.
- Migration of existing rule base to the new devices, NATing, creation of rule base before go-live.
- The solution proposed should be compatible and seamlessly integrated with the existing campus LAN and Internet infrastructure.
- The solution should have high availability features to ensure that systems will be available at any time of the day. The standby firewall (same make and model) for HA should be configured with all policies so that the same can be up when the primary one is down for any reason.
- Highly scalable enterprise class solution. Solutions with limited scalability would not be acceptable to IITP. Solutions which are not mature for over 1 year should not be quoted.
- Creation of DMZ to ensure that the critical corporate data remain protected from cyber threats.
- Smooth & Knee-jerk free removal of the existing firewall from the existing network.

- Seamless Integration with existing security devices and tools present and future tools planned for procurement.
- The proposed firewalls should be able to perform the Link Aggregation function for connectivity from three or more ISPs.
- Ability to integrate seamlessly with Active Directory, PIM tool to provide complete user identification and enable application based policy definition per user or group.
- Increase visibility and understanding of application traffic. Eliminate traffic control beyond allow / deny.
- Firewalls need to integrate more granular blocking capability as part of the base product and should go beyond port/protocol identification and move towards integrated service view of traffic rather than merely performing sheet metal integration.
- Enable to create granular security policy definitions per user and groups to identify, block or limit the usage.
- 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. Scan for viruses and malware in allowed collaborative applications, protect environments with social media and internet applications.
- IITP 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. 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.
- Virtual Private Network (VPN) technologies should be part of the solution to provide resilient and flexible site-to-site, client to site connectivity. Should have management tools to deploy, configure and operate the VPNs.
- Identify and control applications sharing the same connection.
- Should be able to intercept, decrypt and re-encrypt SSL/TLS, SSH, and VPN traffic with low performance degradation.
- Decrypt outbound SSL traffic to ensure protection from sniffing etc.
- Enable the same application visibility and control for remote users.
- Deliver the same production throughput and performance with application control active.
- Updates and upgrades should be automated and performed seamlessly with the ability to view and manage remote operations through the central management system.
- 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. It should rapidly identify and block Trojans, viruses, spam, intrusion attempts and other violations of normal protocol communications.
- Should have ability to manage the security environment through intuitive graphical interface which should provide views, details and reports on security health through a comprehensive, centralized security dashboard.
- 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.
- All the equipment (hardware, software) supplied as part of the solution should be IPv6 ready from day one and should support all the protocols.

- Install & configure management, reporting & logging tool to have a centralized and powerful management which should enable IITP to deploy, view and control all firewall activity through a single pane. There should be an ability to automate routine tasks and drill-downs to produce maximum efficiency with minimal effort.
- Bring to notice and ensure relevant compliance to the guidelines and advisories issued from time-to-time by Government bodies like MEITY, CERN, DOT, MoE along with IITP security guidelines and advisories. The management, reporting and log must be aligned with this objective.
- The product and features are certified from internationally or nationally recognised bodies like Internet Computer Security Association (ICSA) and should feature in leaders/top 5 products in relevant domains in internationally or nationally recognised rating bodies like Gartner or equivalent.
- **Service uptime: 99.99%**

# 6. Local Conditions, Site Survey Gap Analysis

It will be incumbent upon each Bidder to fully acquaint himself with the local conditions and other relevant factors at the proposed site which would have any effect on the performance of the contract and / or the cost. For site visits and other information, the bidders may contact Computer Centre (cc_office@iitp.ac.in).

The Bidder is expected to make a site visit to obtain for himself on his own responsibility all information that may be necessary for preparing the bid and entering into contract.

Failure to obtain the information necessary for preparing the bid and/or failure to perform activities that may be necessary for the providing services before entering into contract will in no way relieve the successful Bidder from performing any work in accordance with the RFP/Tender documents.

It will be imperative for each Bidder to fully inform themselves of all legal conditions and factors which may have any effect on the execution of the contract as described in the bidding documents. The Purchaser shall not entertain any request for clarification from the Bidder regarding such conditions.

It is the responsibility of the Bidder that such factors have properly been investigated and considered while submitting the bid proposals and that no claim whatsoever including those for financial adjustment to the contract awarded under the bidding documents will be entertained by the Purchaser and that neither any change in the time schedule of the contract nor any financial adjustments arising thereof shall be permitted by the Purchaser on account of failure of the Bidder to appraise themselves of local laws and site conditions.

- The quantity of items and works mentioned in this EoI are best effort estimation only (at least these estimated items will be required). The supplier/ vendor/ bidder must conduct a physical site survey to create the actual B.O.Q
- Any item required for properly implementing and commissioning the entire solution but missing in the B.O.Q/B.O.M due to poor estimation by the selected bidder must have to be provided without any additional cost impact to IIT PATNA. Hence, the physical site survey and estimation by interested bidders is imperative.
- Interested bidders should visit the site within 10 days of publishing EoI. The bidder will have to take prior appointment at “cc_office@iitp.ac.in” before site survey. The bidder has to verify the photo ID of his employee on his authorization letter on company letter-head and send it to the email given above.
- All Design & configurations should be as per industry best practices.
- The Bidder will provide IITP with the gap identification report along with the necessary solutions to overcome the gaps within the time limit and the time frames. The Bidder will incorporate all the suggestions made by IITP to the gap report.
- The selected bidder will also ensure that gaps pointed out by the audit and inspection team, statutory and regulatory bodies, or any other third party agency engaged by IITP within the project period will be immediately resolved.

# 7. Estimated list of equipment, software and features

**Some salient points about overall solution architecture:**

| | |
|---|---|
| 1 | The architecture should be built on open-standards based protocols and open APIs |
| 2 | The devices in the network should have full IPv6 functionality. |
| 3 | The devices should deliver the lowest possible latency and high throughput. |
| 4 | There should be a resilient architecture through redundant paths and multiple devices. |
| 5 | The architecture should support separate, dedicated data, control, and management planes. |
| 6 | The architecture should support In-service software upgrade, which will allow seamless upgrades with no traffic loss or performance impact. |
| 7 | The device deployment should ensure low power consumption for environmental friendly deployment. |
| 8 | The scope of the work can be suitably modified by the Institute, if deemed necessary. |

| **Sl. No.** | **Items** | **Remarks** |
|---|---|---|
| 1 | Next Generation Firewall (Hardware, softwares, licenses/ subscription etc.) in HA. | |
| 2 | Management Server, Reporting & Log server (Hardware, softwares, licenses/subscription etc.). | |
| 3 | Campus Network and IT services Security Enhancement Add-on solutions like domain and website protection from fishing, masquerading etc, critical data protection, mail and other software services security and protection. | |
| 4 | 24X7 OEM Comprehensive Warranty and Support for 5 years withNBD replacement. | 24X7 support throughout warranty period. |
| 5 | SLA based 8X7 support - Domain experts and ITIL based Remote Service desk for operations support and monitoring. | 8X7 support- SLA based |
| 6 | Required accessories and switches | As per solution requirement |
| 7 | Operations Training | Technical Sysadmin |

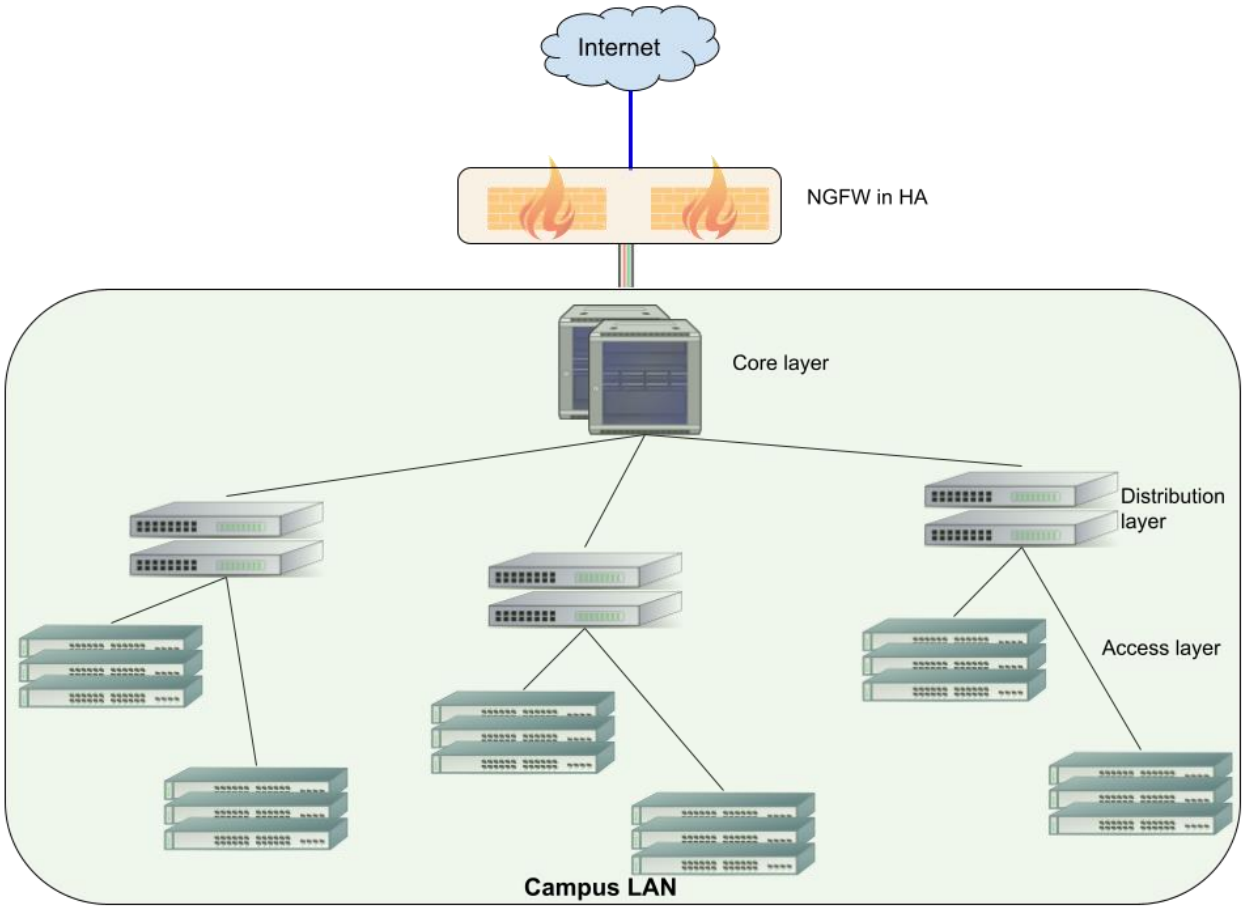


Figure 3: High Level design of NGFW

The high-level list of desired features in the Next Generation Firewall is given below. This list is indicative and bidders are encouraged to present solutions with comprehensive features and services.

- **Centralized Monitoring & Reporting :**

The proposed solution must have a separate management solution for management, logging and reporting to help IITP in log analysis, policy management, firewall rules set export, rules & policy configuration and also to provide administrators with a security health dashboard to view the happenings and traffic patterns and associated risks in the network in real time. A centralized system should enable to deploy, view and control all firewall activity through a single pane of glass. Central management should also give you the ability to automate routine tasks, reuse elements and employ shortcuts and drilldowns to produce maximum efficiency with minimal effort. It should include Web Based reporting, Monitoring & Logging, Monitoring suspicious activity and alerts, Graphical real-time and historical monitoring, email notification of reports, viruses and attacks reports. The reporting tool must ensure user friendly and customized report extraction, IPS, Web filter, Antivirus, Anti-spam system reports, IP and User basis report, various Compliance reports and reasonable no. of drilled down reports. For an external reporting solution, if separate hardware is needed then it should be mentioned clearly.

- **User & Application Control:**

It should be able to identify, allow, block or limit applications regardless of port, protocol to provide visibility into unknown & proprietary applications within IITP's network. It should empower to create detailed policies that can be based on characteristics such as user identity, user role and specific aspects of a web application. It should have more advanced user and application controls such as the ability to

expand user groups, domain names and TLS matches, as well as detailed user and application usage information in reports, logs and statistics.

- **Third-party identity management integration :**

It should support all major authentication protocols such as LDAP/AD, RADIUS, Kerberos and Local Authorization thereby helping organizations control not only the types of traffic that are allowed to enter and exit the network, but also what a specific user is allowed to send and receive.

- **Packet filtering:**

It should control network access by monitoring outgoing and incoming packets and allowing them to pass or halt based on the source and destination Internet Protocol (IP) addresses, protocols and ports. It must support Identity awareness for granular control of applications by specific users, groups of users and machines that the users are using.

- **Deep Packet Inspection:**

It should have the capability to examine the data part of a packet as it passes through it, searching for protocol non-compliance, viruses, spam, intrusions, or defined criteria to decide whether the packet may pass or if it needs to be routed to a different destination, log servers etc. It must ensure the various pieces of each packet are thoroughly examined to identify malformed packets, errors, known attacks and any other anomalies. DPI can rapidly identify and then block Trojans, viruses, spam, intrusion attempts and any other violations of normal protocol communications.

- **IDS/IPS:**

The device must have both inbuilt Intrusion Detection System and Intrusion Detection System. It may be either or all of the signature-based, statistical anomaly-based, and stateful protocol analysis. It must be able to detect and prevent the network efficiently from different kinds of attacks like TCP/IP attack, HTTP attack, email attack, FTP Attack, DNS Attack, ICPM Attack, DOS and DDOS Attack, Telnet Attack. It should have enough signatures. IPS Policies: Multiple, Custom, User-based policy creation, Automatic real-time updates from CR Protect networks, Protocol Anomaly Detection.

- **TLS/SSL traffic inspection:**

The proposed solution should be able to effectively monitor SSL and http tunneled traffic flows. In order to secure encrypted traffic the proposed NGFW must support all inbound and outbound SSL decryption capabilities to help IITP identify and prevent threats and malware in encrypted network streams.

- **QoS/bandwidth management:**

It should have application and user identity based bandwidth management, Multi WAN bandwidth reporting, Guaranteed and Burstable bandwidth policy. Bandwidth for User, Zone, Group, Firewall Rule, URL and Applications to prioritize network traffic by ensuring control of traffic flows on the network so that traffic does not exceed network capacity and thereby resulting in network congestion and also allows to allocate bandwidth for certain types of traffic and also for applications and users.

- **Link Aggregation:**

The appliance proposed should have the capability for Link aggregation. The platform should support the standards based Link aggregation technology (IEEE 802.3ad) to achieve higher bandwidth

- **Network- and port-address translation (NAT):**

It should be capable of allowing NATing & PATing for various purposes as per the requirement. All the equipment (hardware, software) supplied as part of the solution should be IPv6 ready from day one and should support all the protocols.

- **Virtual private network (VPN) :**

IPsec, L2TP, PPTP and SSL as a part of Basic Appliance, VPN redundancy, Hub and Spoke support, 3DES, DES, AES, MD5,SHA1 Hash algorithms, IPsec NAT Transversal.

- **Antivirus Inspection & Anti Bot:**

The NGFW should be able to protect the network from Virus, Worm and should have the ability of Trojan Detection and Removal, Automatic Virus signature database update, Real-Time blacklist, Zero hour Virus outbreak protection. It should have an inbuilt antivirus engine and be able to inspect https traffic on the fly for any infected file and also for protocols like HTTP, HTTPS, FTP, POP3, SMTP, SMB etc. It should also be capable of identifying malware coming from incoming file and malwares downloaded from internet

- **Stateful inspection:**

Solution should track the connections from layer 2 to layer 7 to allow a lot more control and provide IITP with the ability to have very granular policies.

- **High Availability:**

It must have high availability features i.e, Active-Active, Active-Passive as well as Cluster to provide resiliency to the business etc.

- **Integration with security devices:**

The device should be able to seamlessly integrate with other standard security solutions such as SIEM tools, reporting tools, two factor authentication systems etc. with little or no modifications and thereby enhance the overall capability of the security system. Configuration/integration for log correlation with standard SIEM tools like Arcsight, RSA, QRadar etc and syslog servers like Solarwinds etc.

- **Web Filtering:**

It should screen an incoming Web page to determine whether some or all of it should not be displayed to the user. This filter would check the origin or content of a Web page against a set of rules for the Web filter.

- **Advance Persistence Threat Solution:**

Advanced Threat Protection (Detect and block network traffic attempting to contact command and control servers using multi-layered DNS, AFC, and firewall).

- **Sandboxing:**

Solution should inspect executables and documents containing executable content including .exe, .com, .dll, .docx, rtx, etc , Should support dynamic malware behavior analysis run files in real environment.

- **Load Balance:**

For Automated Failover/Failback, Multi-WAN failover, WRR based Load Balancing.

- **High availability:**

Active-Active. QoS, OSPF, RIPv2, BGP, Policy routing based on Application and User support Round Robin Load Balancing.

- **Two Factor Authentication:**

Solution should support the option to integrate with Email/SMS/token based 2FA for Internal as well as VPN users authentication.

## OEM's qualification criteria

| Sl. No. | Criteria (The applicants must satisfy all the criteria) | Compliance (Yes/No) |
|---|---|---|
| 1 | Technical compliance to be provided on OEMs letterhead with signatures, name, email, contact number of Authorized signatory. | |
| 2 | Products should be quoted with Next Business Days (NBD) replacement warranty. | |
| 3 | Quoted products should have 24x7x365 comprehensive Support. | |
| 4 | All categories of Network Switches, Transceivers & Switch OS should be from the same OEM for OEM certified. | |
| 5 | OEM must be a declared leader in nationally or internationally accepted ratings like Gartner. | |

| General Requirements: | Compliance (Yes/No) |
|---|---|
| **Operating Conditions:**<br>All the equipment, components must have the operating conditions aligned to the deployment location like weather, temperature, humidity etc. or proper arrangements must be made to ensure the appropriate operating conditions. | |
| **Seamless Integration with backbone network:**<br>It should seamlessly integrate with the existing network backbone and infrastructure locally (Bidder is entirely responsible for gathering such information in a comprehensive manner). | |
| **Dashboard, UI and reporting** | |
| **Warranty and Support:**<br>● Bidders must produce a comprehensive OEM warranty certificate for the warranty period mentioned in the NIQ/Tender document. Only OEM warranty will be acceptable.<br>● Online OEM portal for product and warranty details along with support and complaint facilities. The supplied items warranty & support will be started after commissioning and acceptance of work.<br>● Escalation matrix<br>● Comprehensive OEM support (including installation and deployment) and maximum 24 hrs. problem/ issue resolution.<br>● Valid Manufacturer's Authorization Form (MAF) (Duly attested hard copy must be submitted with the bid documents.) bearing NIQ/Tender No.<br>● OEM must have 24*7*365 operational support center to address and rectify the issue/problems occurring during the entire warranty period. Latest software upgrade for all products should be available free of charge without any additional cost during the warranty. | |
| **EoS/EoL:**<br>The comprehensive declaration of EoS/EoL for all the equipment must be provided on the OEM letterhead.<br>The supplied components should have End of Life (EoL) at least 5 years from post installation (Proper Certificate from OEM to be attached with bid document). | |

# 8. SRS and Gap Analysis

The bidder/OEM must analyze the existing production system and gather performance metrics. The bidder/OEM 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. The Bidder is also expected to provide suitable Business Continuity Planning applicable to the proposed solution in case the said solution is unavailable at any time or any site. The steps may be as follows:

- Study of existing security architecture, existing firewall & IPS policies & propose enhanced security architecture as per best practice.
- Prepare migration plan for existing firewall & IPS policies along with Next Generation security features mentioned in technical specification.
- Give formal presentation to the IITP security committee on final design, configuration and implementation based on the TAMD document.
- All Design & configurations should be as per industry best practice of NGFW.
- Prepare a plan for all latest stable hotfix to be applied on NGFW
- Prepare the TAMD document and submit it to IITP.
- Get signoff for all User Acceptance Tests from IITP.
- The Bidder will provide IITP with the gap identification report along with the necessary solutions to overcome the gaps within the time limit and the time frames. The Bidder will incorporate all the suggestions made by IITP to the gap report.
- The selected bidder will also ensure that gaps pointed out by the audit and inspection team, statutory and regulatory bodies, or any other third party agency engaged by IITP within the project period will be immediately resolved.

# 9. Project Management and Implementation

The bidder would be responsible, but not limited, to perform the following activities during the installation:

- Checking site readiness for integration
- Meet all plans, specifications and applicable codes and regulatory requirements.
- Installation, deployment and integration of all the hardware and software components of the solution.
- Installation of all the accessories, cable and connectors
- Bunching, dressing and labeling of the cables
- Detailed project documentation (operational, functional and technical), troubleshooting manuals, FAQs, end user manuals etc.
- Project Sign off
- Certification
- Develop and implement a quality control system for the project.
- Coordinate with all the stakeholders to ensure that the project design and schedule is met.
- Coordinate with the General Contractor (and all other appropriate groups) on any infrastructure issues arising during construction, including: scheduling, finishes, clarifications, and identified deficiencies.
- Adherence to design specifications, in case of any deviation the same has to be conveyed to design team
- Coordinate with design team for all design related queries
- Submit regular progress reports to project management team
- Adhere to quality of work during the implementation.
- Establish and maintain on site a complete file of all drawings and items submitted.
- Distribute meeting minutes following each progress meeting.
- Coordinate the preparation of punch lists and ensure that all items are completed on a timely basis.
- Adhere to all safety measures at site during implementation.

## 8.1 Kick-Off

The start of the project implementation will be marked by a Project Kick-off meeting. This meeting will act as a launch pad for the entire project. The project team of selected bidders should be present during the kick-off meeting. During the kick-off, the implementation related details, stakeholders, project plans etc will be discussed.

## 8.2 Go-Live

The Go-Live happens to be one of the most important milestones wherein, all the components of the project have been implemented and integrated in all respects and the entire solution is operational. At this stage, the solution is ready for use and acceptance testing.

## 8.3 Commissioning

This milestone marks final acceptance of the solution by IIT Patna. By this time, all the items in scope of works must be completed with proper documentation and sign-off. This milestone also marks the

start of the support, warranty and maintenance phase. All the components (Hardware/Software etc), remain under the responsibility of the selected bidder until this milestone.

## 8.4 Acceptance testing

The acceptance test cases and schedule will be provided by the selected bidder covering all requirements and components. The test cases, procedures and plans should be accepted by IIT Patna and then testing will be conducted accordingly.

On successful completion of installation, commissioning, acceptability test, receipt of deliverables, training & handholding etc, and after the solution runs successfully for three months after "Go-Live" milestone and IIT Patna is satisfied with the working on the system, the acceptance certificate (as mutually decided and approved by IIT Patna) duly attested and signed by the selected bidder and IIT Patna will be issued.

## 8.5 Training and handholding

**End-User Training:**

The selected bidder for implementation must conduct end-user training to familiarize the end-users with the features available in the solution. The schedule and content of such training must be prepared by the bidder and shared with IIT Patna. This training must be supported with the detailed end-user manuals, help documents, FAQs etc.

**Technical Training:**

The selected bidder for implementation must conduct detailed technical training for the various components of the solution for the technical team of IIT Patna. This must be supported with detailed technical documentation with diagrams, configurations, connectivity and interface details, technical references and literature etc. Furthermore, a demo test bed setup should be a part of this training.

**Operational Training:**

The selected bidder must provide handholding and training support for operational requirements. The operations part must be documented appropriately with steps, configurations, illustrative practical use cases etc.

# 10. Warranty and Support

- The vendor warrants that the products supplied under the Contract are of the most recent version and that they incorporate all recent improvements in design and/or features. The vendor further warrants that all the Products supplied under this Contract shall have no defect, arising from design or from any act of omission of the vendor that may develop under normal use of the supplied products in the conditions prevailing in India.
- Warranties for OEM products shall be provided on a pass-through basis. There are no implied conditions or warranties.
- The minimum warranty period shall be 5 (Five years) years/ 60 (Sixty) months or as per requirements mentioned in section 5,6 and 7 from the date of commissioning and acceptance of the work in totality. The vendor shall, in addition, comply with the performance guarantees specified under the Contract. If, for reasons attributable to the Selected applicant, these guarantees are not attained in whole or in part the vendor shall make such changes, modifications and/or additions to the Products or any part thereof as may be necessary in order to attain the contractual guarantees specified in the Contract at its own cost and expense and to carry out further performance tests.
- During the warranty period, the vendor shall repair/replace at the installed site, at no charge to IIT Patna, all defective components that are brought to the Vendor's notice. Warranty should not become void, if IIT Patna buys any other supplemental hardware from a third party and installs it within these machines under intimation to the vendor. However, the warranty will not apply to such supplemental hardware items installed.
- In case of critical non-functioning of any item under warranty, the replacement of equipment has to be done within 48 hours.
- Post commissioning, there will be a SLA based defect liability and hand holding period of Six months wherein the selected bidder will operate the implemented solution and fix any defect arising during this period without any cost impact to IIT PATNA. Any additional equipment required to operate the solution or fix the defects will be bidders responsibility.

# 11. GENERAL TERMS AND CONDITIONS

*01.* ***Rates*:** Rates quoted must be on F.O.R basis for IIT Patna, on DOOR DELIVERY Basis, with break up as per details given in BoQ at the time submitting the tender.

02. ***Validity:*** The validity period of the offer should be clearly specified. It should be valid for at least 180 days from the last date of submission of quotations/proposal/tender.

03. **GST Certificates & TDS:** Scanned Copy of GST Certificate must be uploaded with technical bid. Appropriate GST TDS and IT TDS will be applicable.

04. **Dealership Certificate:** Dealership certificate (in case of authorised dealers) and standard Technical literature on the offered products must be uploaded with technical bid.

05. **Performance Guarantee:** An amount of 03% of total order value needs to be paid using link https://www.onlinesbi.com/sbicollect/icollecthome.htm?corpID=595859 towards Performance Security/ Guarantee. Performance Security/Guarantee may also be submitted in the form of Bank Guarantee/ Fixed Deposit for such period as to cover two months beyond the AMC/Warranty period for the order.

06. **Late and delayed quotation:** Late and delayed quotations will not be considered in any circumstances.

07. **Ground for Rejection of Quotation:** The quotations are liable to be rejected, if the foregoing conditions are not complied with. The quotation should be complete in all respects. If a firm quotes NIL charges / consideration, the bid shall be treated as unresponsive and will not be considered.

08. **Payment:** Payment will be made on quarterly basis after producing the invoice along with maintenance, uptime, attendance, duty roster, call reports and with ESIC, PFA data of deputed employee duly certified by Head Computer Center. Payment will be made online only. Following information must be clearly written in the uploaded bank details for RTGS/FUND TRANSFER:
    (a) Name of the Firm with complete postal address
    (b) Name of the Bank with Branch where the Account exist
    (c) IFSC CODE
    (d) ACCOUNT No
    (e) PAN No
    (f) GST/TIN No

09. **Liquidated Damage:** If a firm accepts an order and fails to execute the order in part or in full, as per the terms and conditions stipulated in the Purchase Order, it will be open to the institute to recover the liquidated damages from the firm at the rate of 0.5% per week of the order value subject to a maximum of 10% of the order value. It will also be open to the institute alternatively, to arrange procurement of the required stores from any other source at the risk and expense of the defaulter firm/vendor, which accepted the order but failed to execute the order according to the stipulated agreed upon. Defaulter vendor(s)/ firm(s) are also liable for debarment.

10. **Termination for default:** Default is said to have occurred:
    (a) If the supplier fails to deliver any or all of the goods/ items/ services within the time period(s) specified in the purchase order or any extension thereof granted by IIT Patna.
    (b)If the supplier fails to perform any other obligation(s) under the contract
    (c) If the vendor, in either of the above circumstances, does not take remedial steps within a period of 04 days after receipt of the default notice from IIT Patna (or takes longer period in-spite of what IIT Patna may authorize in writing), IIT Patna may terminate the contract / purchase order in whole or in part.

11. **Applicable Law:**
    (a)The contract shall be governed by the laws and procedures established by Govt. of India, within the framework of applicable legislation and enactment made from time to time concerning such Commercial dealings / processing, as may be applicable upon IIT Patna.
    (b)All disputes are subject to exclusive jurisdiction of Competent Court and Forum in Patna, India only.
    (c) Any dispute arising out of this purchase shall be referred to the Registrar IIT Patna, and if either of the parties hereto is dissatisfied with the decision, the dispute shall be referred to an Arbitrator, who should be acceptable to both the parties, (to be appointed by the Director of the Institute). The decision of such Arbitrator shall be final and binding on both the parties.

12. **Important:** The Director may accept or reject any or all the bids in part of in full without assigning any reason and doesn't bind himself to accept the lowest bid. The institute at its discretion may change the quantity / upgrade the criteria / drop any item, at any time before placing the Purchase Order.
13. **Force Majeure:** The Supplier shall not be liable for forfeiture of its performance security, liquidated damages or termination for default, if and to the extent that, it's delay in performance or other failure to perform its obligations under the Contract is the result of an event of Force Majeure.

    (i) For purposes of this Clause, "Force Majeure" means an event beyond the control of the Supplier and not involving the Supplier's fault or negligence and not foreseeable. Such events may include, but are not limited to, acts of the Purchaser either in its sovereign or contractual capacity, wars or revolutions, fires, floods, epidemics, quarantine restrictions and freight embargoes.

    (ii) If a Force Majeure situation arises, the Supplier shall promptly notify IIT Patna in writing of such conditions and the cause thereof. Unless otherwise directed by the Purchaser in writing, the Supplier 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.
14. It is the sole responsibility of the vendor to comply with all labor laws applicable during execution of service/AMC in IIT Patna for safeguard of their employees.
15. IIT Patna will deduct statutory taxes applicable at the time of making payment to the vendor from regular Bill/Invoice of the vendor and only net payment will be released to the vendor.
16. If agency does not complete assigned job as per the satisfaction of IIT Patna, IIT Patna will engage some other agency for completion of work and actual expenditure incurred by IIT Patna will be recovered from the due payment of AMC charges.
17. The "in general Printed conditions" of supply of the firm, if any, will not be binding on the Institute.
18. The bidders can quote only those products in the bid which are not obsolete in the market and has at least 3 years residual market life. Moreover, the bidders are bound to supply the spares till 10 years from the date of installation, on the same payment terms.
19. The bidders can quote only items with minimum 20% domestic value additional/local content. Local content means the amount of value added in India which shall be the total value of the item procured (excluding net domestic indirect taxes) minus the value of imported content in the item (including all custom duties) as a proportion of the total value, in percentage. The bidders are required to furnish a self-certificate regarding the items meeting local content requirement, mandatorily mentioning following:
    a. Percentage of Local Content
    b. Location(s) at which the local value addition is made.
20. 'Class-I local supplier' shall get purchase preference over 'Class-II local supplier' as per instructions contained in Public Procurement (Preference to Make in India) Order 2017, as amended from time to time. The margin of purchase preference shall be 20%.
21. Any bidder from other countries (outside India) is not eligible to bid in this tender. Bidder for the purpose of this clause means:
    a. Any entity incorporated, established or registered outside India; or
    b. A subsidiary of an entity incorporated, established or registered outside India; or
    c. An entity substantially controlled through entities incorporated, established or registered outside India; or
    d. An entity whose beneficial owner is situated outside India; or
    e. An Indian (or other) agent of entity incorporated, established or registered outside India; or
    f. A natural person who is a citizen of other countries; or
    g. A consortium or joint venture where any member of the consortium or joint venture falls under any of the above (a to f).

# 12. Documents to be submitted

**A. General Documents:**

1. Scanned copy of bank details for NEFT/RTGS on letter head and certificate of GST.
2. Scanned copy of self-declaration of original manufacturer or authorized dealership certificate from OEM.
3. Scanned copy of self-certificate regarding the items meeting local content requirement as mentioned in clause 20 of general terms and condition.

**B. Duly filled, signed and stamped Form-1 to Form-5.**

**C. EoI Specific Documents:**

1. Prequalification/Essential Eligibility criteria and supporting documents
2. Copy of the certificate of registration of the firm
3. Copy of the Company profile.
4. Documents supporting all the details for information provided above.

**D. Technical Documents**

1. Solution and Architecture to Scope of work mentioned in section 5.
2. Duly attested Detailed Unpriced BOM/BOQ for the Solution based on section 5, 6, 7 and 8.
3. Compliance, test reports and supporting documents to Minimum Technical requirements mentioned in section 7.
4. Integration with existing Campus Data and telephone network.
5. End-of-sale, end-of-life and end-of-support details for each component of the solution.
6. Product literature and data sheets.
7. User friendly and innovative features.
8. Scalability w.r.t. future expansion and integration of new technologies.
9. Management and monitoring.
10. Project Management-section 8
11. Warranty and support details, methodology, and plan with well defined SLAs and escalation matrix-section 9.

# Form-1

## TENDER/EoI ACCEPTANCE LETTER

**(To be given on Company Letter Head)**

To,
The Registrar,
(for Stores & Purchase Section)
Indian Institute of Technology Patna
Kanpa Road, Bihta, Patna, Bihar-801106
Phone: 06115-233-683

**Sub: Acceptance of Terms & Conditions of Tender/EoI**.

**Tender/EoI Reference No.:_____**

**Name of Tender/Work/EoI:-**

_____

_____

Dear Sir/Madam,

1. I / We have downloaded / obtained the tender/EoI document(s) for the above mentioned "Tender / Work/EoI" from the website(s) namely: _____ as per your advertisement, given in the above-mentioned website(s).
2. I / We hereby certify that I / We have read the entire terms and conditions of the tender/EoI documents from Page No. _____ to _____ (including all documents like annexure(s), schedule(s), etc.), which form part of the contract agreement and I / we shall abide hereby by the terms / conditions / clauses contained therein.
3. I/We have read the clause 22 of General Terms & Conditions, regarding restrictions on procurement from a bidder outside the country; I/We certify that this bidder is from India. I/We hereby certify that this bidder fulfills all requirements in this regard and is eligible to be considered.
4. The corrigendum(s) issued from time to time by your department / organizations too have also been taken into consideration, while submitting this acceptance letter.
5. I / We hereby unconditionally accept the tender/EoI conditions of above-mentioned tender/EoI document(s) / corrigendum(s) in its totality / entirely.
6. I / We do hereby declare that our Firm has not been blacklisted / debarred by any Govt. Department / Public Sector Undertaking.
7. I / We certify that all information furnished by our Firm is true & correct and in the event that the information is found to be incorrect/untrue or found violated, then your department / organization shall without giving notice or reason thereof or summarily reject the bid or terminate the contract, without prejudice to any other rights or remedy including forfeiture of the full said EMD absolutely.

**Yours Faithfully,**

**(Signature of the Bidder, with Official Seal)**

Email ID: …….

Phone no.: ……

Mobile no.: ……..

Address for notice: ……..

## Form-2

## STRUCTURE & ORGANIZATION

| | |
|---|---|
| Name & Address of the applicant | |
| Telephone No.<br>Telex No.<br>Fax No. | |
| Particulars of registration with various Government bodies (attach attested photocopy)<br>a. Organization/Place of Registration<br>b. Registration No. | |
| Name and Titles of Director & Officers with designation to be concerned with this work | |
| Designation of individuals authorized to act for the organization | |
| Has the applicant ever abandoned the awarded work before its completion? If so, give the name of the project and reasons for abandonment. | |
| Was the applicant ever required to suspend assignment for a period of more than six months continuously after commencement of the assignment? If so, give the name of the project and reasons for suspension of work. | |
| Has the applicant ever been debarred / black listed for tendering in any organization at any time? If so, give details. | |
| Has the applicant ever been convicted by a court of law? If so, give details | |
| Any other information considered necessary but not included above | |

## Form-3

Applicants must furnish annual financial statements for the last five years in Form_____.

## FINANCIAL INFORMATION

I. Financial Analysis – Details to be furnished duly supported by figures in balance sheet/profit and loss account for the last five years duly certified by the Chartered Accountant, as submitted by the applicant to the Income Tax Department (copies to be attached).

| | Financial Year | | |
|---|---|---|---|
| Particulars | 2018-19 | 2019-20 | 2020-21 |
| (i)Gross Annual Turnover (In Lakhs Rupees) | | | |
| (ii) Profit/Loss (In Lakhs Rupees) | | | |
| (iii)Income from IT service and solutions (In Lakhs Rupees) | | | |

a) Current Profit & Loss account

Signature of Chartered Accountant with seal Signature of Applicant(s)

## Form-4

## DETAILS OF ASSIGNMENTS PROJECTS OF SIMILAR NATURE COMPLETED DURING THE LAST FIVE YEARS ENDING <Date>

| Sl. No. | Description | Project Details |
|---|---|---|
| 1 | Name of work/project and Location | |
| 2 | Project Objectives | |
| 3 | Name & Address of Employer/organization | |
| 4 | Cost of work in INR. | |
| 5 | Complexity of the task (modules, etc.) | |
| 7 | Date of commencement as per contract | |
| 8 | Stipulated date of Completion | |
| 9 | Up to date percentage progress of work | |
| 10 | Slow progress if any and reasons thereof | |
| 11 | Name and address/email and telephone number of officer to whom reference may be made. | |
| 12 | Remarks | |

* For each work, a separate sheet be prepared.
* For each work, a duly attested performance report must be provided.

Signature of Applicant(s) with date & seal

# Form-5

## Document Check-List

| Description | Yes/No |
|---|---|
| 1. Proposal for EOI | |
| 2. All the documents listed in documents section 11 along with supporting documents | |
| 3. Is the document is in pdf only | |
| 4. If any other information (not called for in Form _____) is furnished, it is in A4 size sheets, endorsed with seal and signature of the applicant along with date of submission on every page | |
| 5. All corrections are neatly crossed out, rewritten, initialed with date | |
| 6. Pages of the documents are numbered as "page m of n" | |
| 8. Each page of the application is signed | |
| 9. There are no .ppt or .xls files embedded or attached. | |
| 10. References, information & certificates from clients are signed by authorized persons. | |