INDRAPRASTHA INSTITUTE *of*
INFORMATION TECHNOLOGY
DELHI

TENDER FOR SUPPLY & INSTALLATION OF NEXT GENERATION FIREWALL FOR CAMPUS OF THE INSTITUTE AT OKHLA PHASE-III, NEW DELHI-110020

(IIIT-D/IT/NGFW/013/2022-23)

INVITATION FOR BIDS

Indraprastha Institute of Information Technology -Delhi (IIITD), a State University created by an Act of Govt. of NCT of Delhi, invites sealed bids for **Supply and installation of Next Generation Firewall** (as per specifications mentioned under Scope of Work below) for its campus at Okhla Phase-III New Delhi-110020.

1. An amount of Rs. 1,00,000/- (One Lakh only) towards earnest money (EMD) must be deposited in the form of demand draft in favour of "IIIT-Delhi Collections" account, payable at New Delhi. No interest will be paid on the earnest money deposited by the bidder. Tender Document without earnest money will be summarily rejected.EMD is exempted for MSMEs/NSIC registered suppliers

2. The tender document can be downloaded from the Institute's website. Those wishing to get the copy of the document from the Institute may please deposit a non-refundable Tender Document Fee of Rs.1, 180/- (Rupees One Thousand One Hundred Eighty only) in the form of Demand draft drawn in favour of IIIT-Delhi Collections", payable at New Delhi or may deposit Rs.1, 180/-with the F&A division of the Institute and enclose the receipt with the filled up tender document. The tender fee is exempted for MSMEs/NSIC registered suppliers.

3. The last date for submission of Bid is 12th October 2022 up to 3:00 PM. The Technical Bids shall be opened on the same day, i.e., on 12th October 2022 at 3.30 PM. The Tender Document should be addressed to:

Registrar,
Indraprastha Institute of Information Technology-Delhi
Okhla Phase-III
(Behind Govind Puri Metro Station)
New Delhi-110020.

The document should be deposited in the Tender Box kept in the Store & Purchase department in Room no. A 108, First Floor, Old Academic Block of the Institute. Bids received after 3:00 PM will not be accepted or considered under any circumstances.

Note:- The Bidder/Any subsidiary of Bidder and the OEM who was L1 in tender No:- IIIT-D/IT/NGFW/017/2021-22 is not allowed to bid in this tender. Any bid with the L1 OEM w.r.t IIIT-D/IT/NGFW/017/2021-22 will be rejected.

Bidding Procedure:

1. Bids are invited in Two Bids System, i.e. (1) Technical and (2) Financial.

   Technical and Financial bids should be sealed separately and enclosed in a sealed envelope clearly indicating separately Technical Bid for "**Supply and installation of Next Generation Firewall**" and Financial Bid for "**Supply and installation of Next Generation Firewall**" addressed to Registrar IIIT-Delhi, Okhla Industrial Area Phase-III, New Delhi-110020.

2. Sealed quotations shall be received no later than 3.00 PM on 12th October 2022. No bids will be accepted after this date & time under any circumstances. The Institute will not be responsible for any postal/courier delay and reasons beyond the Institute's control.

3. Technical bids must contain the EMD for specified amount, along with complete technical details as desired by this tender. Technical bids of all the tenderers will be opened on pre scheduled date, time & venue. Technical bids without EMD will be summarily rejected. The financial bid will be opened after evaluation of the technical bid. Financial bid of only those meeting the requirement of the Institute will be opened and no representation in this regard will be entertained. The date, time of opening of financial bid will be communicated later. The EMD is exempted for MSMEs/NSIC registered suppliers.

Scope of Work, Technical Eligibility and Technical Specification

1. Supply and installation of Next Generation Firewall (Qty.:-1)

Technical Eligibility	**Compliance (Yes/No)**
Offered OEM's NGFW products must have the presence in last 3 years at IITs/NITs/IIITs [**Copy of Purchase Orders with completion certificate and Reference contact details to be attached**]	
Offered NGFW Product by L1 bidder will be installed at IIITD campus for initial period of 2 months on evaluation basis. If IIITD finds the offered product's performance satisfactory then payment will be released. If there are major issues found or product not performing as per the technical specification mentioned in the RFP then IIITD will cancel the order and will contact L2 bidder/OEM product for the same and so on.	
The offered NGFW Product/appliance should not be declared End of Sales/End of Life/End of support on or before the last date of the bid submission. [**A Declaration from the OEM must be enclosed**]	
Offered Product must be supported for at least 7 years (Seven Years) from the date of installation w.r.t technical support, hardware replacement and firmware, Web filter, application filter, Antivirus, IPS/IDS signature, sandboxing updates. [**A Declaration from the OEM must be enclosed**]	
The offered NGFW product should be capable of providing firewall, application visibility, and IPS, antivirus functionality in a single appliance.	
Offered Next Generation Firewall & IPsec should be ICSA Lab certified	
Offered Next Generation Firewall should be Common Criteria (CC) Certified.	
Offered NGFW product and its software and services/portal/any management tool should be from same OEM. Any open source and third party solution is not accepted.	
Offered OEM will provide 24x7 support on call, on email and also provide response in 4hrs of ticket raise. In case of hardware failures replacement should be provided on next business day.	
The offered NGFW product have to be proposed with 3 Years of support bundle with 24x7x365 days TAC support, RMA, HA License, software updates and subscription update support. The NGFW must be proposed with 3 years subscription licenses for NGFW, NGIPS, Anti-Virus, URL Filtering, Anti Spyware, Anti Botnet, Anti APT and SSL VPN Users License.	
Offered OEM will provide publicly accessible and authentication based web portal login to log, track technical support tickets and its status.OEM will also provide publicly accessible and authentication based web portal login to track warranty status, provided support and subscription status of the offered NGFW product.	

Selected bidder/OEM has to install, configure/migrate policies, routing and do the complete migration of the internal and external traffic on the offered NGFW product as per the directions given by the IIITD officials.	
A Training and hands on session have to be provided by the selected OEM to the IIITD officials on the offered NGFW product w.r.t to operation, management, troubleshooting and best practices.	
IIITD can use any performance measurement tools and software, hardware to verify the offered NGFW/firewall appliance performance. In case of any hardware failure during the performance testing, OEM/bidder has to provide the replacement.	

Features	**Compliance (Yes/No)**	**Offered Technical Specs**
Hardware:- I. The offered NGFW Solution should be supplied with at least 8x 1GE RJ-45 interfaces and 8x 10G SFP+ SR interfaces slot, 4x 40GE QSFP slot, 4x 1G SFP slot or if offered 10G SFP+ can work on 1Gbps then no need to offer separate 4x 1G SFP slots.8x10G SFP+ SR and 4x40GE QSFP+ SR transceiver should be provided and 4x 1G SFP optical transceivers should be provided if offered SFP+ transceivers can't work on 1Gbps Console and management ports to access device in case of no network availability II. Console and management ports to access device in case of no network availability III. Appropriate energy efficient redundant (N+N) hot swappable power supplies. IV. The NGFW product should be a multicore CPU architecture with a hardened 64-bit operating system(**A document of the proposed hardware architecture must be attached**) V. Any accessory to mount the unit in rack and power cables should be provided.		
Performance and Throughput(IPv4,IPv6):- i. **NGFW:-** 15Gbps or higher ii. **Threat Protection:-** 15Gbps or higher iii. **IPS Throughput:-** 20Gbps or higher iv. **SSL-VPN Throughput:-** 15Gbps or higher v. **IPsec VPN Throughput:-** 25Gbps or higher vi. **Firewall: -** 50Gbps of throughput on 64 byte packets. Performance should not degrade while IPv6 is enabled in future vii. **Concurrent sessions:-** At least 20 Million, expandability should be provided to expand it to 32 Million viii. **Sessions per second:-** 5,50,000 or higher ix. **VLANs**- At least 1000 VLANs should be supported x. **VPN users**- At least 1000 concurrent VPN users should be supported Any additional performance offered please specify and attach document for the same **A support document must be attached for the offered performance and the throughput**		
General Requirement:- i. Offered NGFW product should provide application detection for DNS, FTP, HTTP, SMTP,ESMTP, LDAP, MGCP, RTSP, SIP, SCCP, SQLNET, TFTP, H.323, SNMP		

ii. Offered NGFW product should support creating access rules/policies with IPv4 & IPv6 objects simultaneously iii. Offered NGFW product should support operating in routed & transparent mode. Both modes can also be available concurrently using Virtual Contexts. Minimum 10 virtual firewall license to be provided from day 1 iv. Offered NGFW product should support Static, Policy route, RIP, OSPF, OSPFv3 and BGP routing protocols v. Offered NGFW product should support manual NAT and Auto-NAT, Static NAT, Dynamic NAT, Dynamic PAT vi. Offered NGFW product should support NAT66 (IPv6-to-IPv6), Nat 64 (IPv6-to-IPv4),NAT46/NPTv6 (IPv4- to-IPv6) DNS64 & DHCPv6 functionality vii. Offered NGFW product should support Multicast protocols like IGMP, PIM, etc. viii. Offered NGFW product should support security policies based on group names in source or destination fields or both. ix. Offered NGFW product should support capability to limit bandwidth on basis of apps, groups, networks, geo locations, ports, etc. x. Offered NGFW product should be supplied with 1500 or more SSL VPN users license xi. Offered NGFW product's Security control (like Firewall, antivirus, IPS, web filtering, application filtering,) must not have any licensing restriction on the number of users. xii. Offered NGFW product should support Dual Stack with IPv4 and IPv6 functionality. xiii. Offered NGFW product should support Sandboxing(Zero day threat prevention) xiv. Offered NGFW product should support network traffic classification which identifies applications across all ports irrespective of port/protocol/evasive tactic. xv. Offered NGFW product must allow policy rule creation for application control, user-based control, host profile, threat prevention, Anti-virus,file filtering, content filtering, QoS and scheduling using single web based dashboard. xvi. Offered NGFW product should be able to handle, alert, block or allow/deny unknown / unidentified applications like unknown UDP & TCP xvii. Offered NGFW product must provide web based management interface xviii. Offered NGFW product must have VPN clients for Windows, Linux(Ubuntu, Redhat), MacOSx, Android, IOS operation systems If any addition features offered please mention		
Management/Monitoring, Logging, Reporting and Log Analyser:- i. Management must be accessible via a web-based interface by any browser. ii. Management interface should have Dashboard to provide real-time status such as: - CPU and memory usage, date, time, subscription and support status, bandwidth utilization, traffic overview, threats etc. iii. Management solution must be capable of role-based administration iv. Management shall provide the functionality of Auto-Check for latest firmware/software versions &		

download the same manually as well as automatically if configured. v. Management engine should block login from the IP if certain failed numbers of login attempted vi. Management engine should provide the feature to allow administrator login from certain whitelisted IPs vii. Management should also be accessible over SSH viii. Management system should provide logging, and reporting and basic event correlation functionality. ix. Management interface should be customizable. x. There should be support for SNMP monitoring xi. Logging should be provided to log all the traffic xii. Logging should be provided to log all the configuration changes done by administrator and the IP address used to login. xiii. Logging should provide to log the user logins including VPN logins. xiv. Stored Logs should be accessible for a period of a month on the offered device internal storage. xv. Logging feature should have separate real time logging based on all Traffic, Threats, User IDs, Data filtering, Content filtering, unknown malware analysis, Authentication, Tunnelled Traffic and correlated log view based on other logging activities. xvi. The proposed NGFW product should provide and support the Comprehensive event logging, Historical Reporting, Report generation, Syslog, Centralized log analyser, Email Notification. xvii. The proposed NGFW shall have logs populated with end user activity reports for site monitoring within the local firewall and Analyser. xviii. Proposed NGFW shall be capable of sending daily scheduled reports over email to the administrators. xix. A Separate Log analyser (virtual machine or physical hardware) should be provided to store logs from NGFW. This log analyser should be capable of handling 25GB logs per day. And should be capable of storing the logs for one year. There should be provision to increase the handling of logs per day. xx. There must be support in NGFW and log analyser for multiple report formats, such as PDF, and CSV xxi. Offered reporting system should provide hits against firewall rules to provide usability and information on utilization of rules in access Policies. xxii. The offered NGFW and log analyser must provide robust reporting capabilities, including a selection of pre-defined reports and the ability for complete customization and generation of new reports. xxiii. The NGFW and log analyser should offer reports that can be generated based on various factors such as Source / Destination IP Address, TCP/UDP Port Number, Protocol, ID, applications,URLs, Traffic flow between the Zones, Timestamp, Human readable description of event and action taken etc. xxiv. The offered NGFW product reporting system should be able to link Active Directory and/or LDAP usernames to IP addresses related to suspected security events. xxv. The offered NGFW product must include an integration mechanism, preferably in the form of open APIs and/or standard interfaces, to enable events and log data to be shared with external		

network and security management applications, such as Security Information and Event Managers (SIEMs), and log management tools. Any other feature/advanced feature w.r.t Management/Monitoring, Logging, Reporting and Log Analyser is offered please specify.		
Authentication:- i. Offered NGFW product must be able to connect with LDAP,Winodws Active directory,Radius,Kerberos ii. There should be option to authenticate VPN users by LDAP,Windows Active directory iii. The NGFW should support to offer an authentication web page which should be authenticated over Windows active directory or LDAP while user tries to connect internet. The authentication page should have a configurable auto renew timer. Any other advanced authentication feature is offered please specify		
High Availability i. Offered NGFW should support Active/Standby and Active/Active failover ii. Offered NGFW should support ether channel or equivalent functionality for the failover control and providing additional level of redundancy iii. Offered NGFW should support redundant interfaces to provide interface level redundancy before device failover iv. Offered NGFW should support 802.3ad Ether channel or equivalent functionality to increase the bandwidth for a segment.		
Next Generation Firewall:- i. Offered NGFW product must support policy-based forwarding based on zone, source/destination address and port, application, AD/LDAP user or user group and services or ports ii. Should be capable of detecting and blocking IPv6 and IPv4 attacks. iii. The offered NGFW product should have the capability of passively gathering information about virtual machine traffic, network hosts and their activities, such as operating system, services, open ports, client applications, and vulnerabilities, to assist with multiple activities, such as intrusion event data correlation, elimination of false positives, and policy compliance. iv. The offered NGFW product should be capable of automatically providing the appropriate inspections and protections for traffic sent over non-standard communications ports. v. The offered NGFW product should be capable of tuning IDS/IPS sensors (e.g., selecting rules, configuring policies, updating policies, etc.) with minimal human intervention. vi. Offered NGFW solution must have inbuilt Capabilities to identify applications and map them to respective ports OR Offered NGFW product must have inbuilt option for policy optimization to identify port-protocol and		

application based policies. For example-Firewall is configured with Security policy to allow port 80/443 and multiple applications (Facebook/Rapid share etc.) traffic going through the same policy, then the firewall should automatically identify those risky applications and reduce the attack surface area vii. The offered NGFW must provide IP reputation feed that comprised of several regularly updated collections of poor reputation of IP addresses determined by the proposed security OEM viii. The offered NGFW should support URL and DNS threat feeds to protect against threats ix. The NGFW OEM must have its own threat intelligence analysis centre and should use the global footprint of security deployments for more comprehensive network protection. OEM shouldn't use 3rd party IPS,AV engines. x. The offered NGFW's detection engine should support capability of detecting and preventing a wide variety of threats and new threats (e.g., malware, network probes/reconnaissance, VoIP attacks, buffer overflows, P2P attacks, etc.. xi. Offered NGFW should be able to identify attacks based on Geo-location and define policy to block on the basis of Geo-location xii. The offered NGFW's detection engine must incorporate multiple approaches for detecting threats, including at a minimum exploit-based signatures, vulnerability-based rules, protocol anomaly detection, and behavioural anomaly detection techniques. xiii. The NGFW must have the capability to create DOS prevention policy to prevent against DOS attacks on per zone basis (outbound to inbound, inbound to inbound and inbound to outbound) and ability to create and define DOS policy based on attacks like UDP Flood, ICMP Flood, SYN Flood (Random Early Drop and SYN cookie), IP Address Sweeps, IP Address Spoofs, port scan, Ping of Death, Teardrop attacks, unknown protocol protection etc.		
URL/Webfilter,Content filter, Application filter:- i. The offered NGFW product should have the capability to inspect SSL traffic. The SSL inspection throughput should not be less than 15Gbps. ii. Offered NGFW should cater to reputation and category based URL filtering offering comprehensive alerting and control over suspect web traffic and enforces policies in more than 75 categories from day one iii. The proposed NGFW shall have custom URL-categorization iv. The proposed NGFW shall provide customizable block pages v. The URL filtering service should be able to categorize a site by multiple categories and not just a single and custom category vi. NGFW should have URL or URL category base protection from phishing attack with malicious URL path vii. The proposed NGFW should have zero-day malicious website or URL blocking update for URL DB update		

for zero-day malware command and control, spyware and phishing websites access protection viii. The proposed NGFW shall have URL Filtering policies by AD user, group, machines and IP address/range ix. The proposed NGFW should have wide range of application control such as: - QUIC, zoom, crypto currency, cloud, gaming, remote etc. and it should have categories of the applications so the admin can block or allow certain category of the application. The applications signatures should be updated on regular interval. x. The proposed NGFW should support DNS category filtering to control user access to web resources. xi. The DNS filtering solution should have the following features: • Filters the DNS request based on the domain rating. • Should block the DNS request for the known botnet C&C domains. • Should allow to define own domain category. • Should allow users to define own domain list to block or allow. **Optional** • Should support DNS safe search to enforce Google, Bing, and YouTube safe addresses for parental controls. • Should support DNS translation that can map the resolved result to another IP that user can define. If any advanced features offered. Please specify		
IPS:- i. Should support more than 3000 application layer and risk-based controls that can invoke tailored intrusion prevention system (IPS) threat detection policies to optimize security effectiveness. ii. Intrusion prevention signatures should be built based on the vulnerability itself. The signature should be able to stop exploit attempts on a known system or application vulnerability. iii. IPS signatures must be updated on regular interval iv. There should be option to create custom IPS signature If any advanced features offered. Please specify		
Antibot,Antivirus i. The proposed NGFW shall have on box Anti-Virus, Anti Spyware signatures and should have minimum signatures update window of every two hour ii. All incoming and outgoing should be scanned by the engine. iii. The proposed NGFW should be able to perform Anti-virus scans for HTTP,HTTPs smtp, imap, pop3, ftp and SMB traffic with configurable AV action such as allow, deny, alert etc iv. Anti-Virus must be able to stop incoming malicious files v. Anti-Bot protections must be able to scan for bot actions vi. Anti-Bot application must use a multi-tiered detection engine, which includes the reputation of IPs, URLs		

and DNS addresses and detect patterns of bot communications vii. Anti-bot application must be able to detect and stop suspicious abnormal network behaviour If any advanced features offered. Please specify		
Zero Day threat protection i. Advance unknown malware analysis engine with real hardware (dedicated on premises sandbox solution to be provided to assure no traffic go on cloud for any kind of analysis) sand box solution, detecting VM-aware malware to detect and protect from virtual sandbox evading advance unknown malware. Sand box analysis should be done for Windows family OS and applications, Mac OS and applications, Linux OS and applications, Android OS and applications, IOS and applications or The emulation and zero-day inspection should be OS agnostic ii. Offered Sandboxing Throughput should be (VM based) 100 files/Hr., Real-world Effective Throughput (Files/Hr.) 500,Number of VMs 6 , It should provide option to customize VMs with our own Windows and Linux OS, applications or The emulation and zero-day inspection should be OS agnostic. iii. Zero day detection should be notified on the email to the administrator and should be blocked. If any advanced features offered. Please specify		

NGFW Means here:-Next Generation Firewall

2. Supply and installation of one onsite Standby NGFW hardware with above specs but without the subscription.

Note:- Installation, Configuration and Final deployment must be done within 30 days of delivery of the product. . If Bidder fails to do deployment within 30 days of the delivery of the product, a fine of 2000/- Rs per day for the first seven days and @ Rs. 5,000/- per day from the 8th day onwards will be levied.

Minimum Eligibility Requirement:

1 Bidder should be OEM/Authorized Partner/service provider of the OEM. In case the Bidder is an Authorized Partner or Service Provider, a valid Agency-ship/Dealership Certificate (**MAF specific to this Tender**) to quote on behalf of OEM should also be enclosed along with the technical Bid. **A document in support of this must be enclosed.**

2 OEM & Authorized Partner should have Sales and support office in Country. **A self-certified document in support of this must be enclosed.**

3 OEM or Authorized Partner should have a service and support office in Delhi NCR. **A self-certified document in support of this must be enclosed.**

4 The warranty provided by the Bidder should have a back-to-back arrangement with the OEM. **The declaration should be part of a Letter of Authorization and signed by a competent authority at the OEM**.

5 The Bidder should be ISO 9001 certified. **A copy of the ISO Certificate should be enclosed.**

6 The Bidder should have a support centre with a minimum of 3 relevant support engineers. **A self-certified document in support of this must be enclosed.**

7 The vendor/OEM should be able to provide 24x7 NOC & Tele support of their own if required by IIITD at agreed terms. **A self-certified document in support of this must be enclosed.**

8 The Bidder shall provide the Registration number of the firm along with the valid GST number with the PAN Number allotted by the competent authorities. **A self-certified document in support of this must be enclosed.**

9 The Bidder must not be blacklisted by the Central Government, State Government, or Government of Corporations in India. **A certificate or undertaking to this effect must be submitted.**

10 If the Bidder is an authorized partner or service provider of an OEM, **an undertaking from the OEM is required** (please enclose) stating that they would facilitate the Bidder regularly with technology/product updates and extends support for the warranty as well.

11 The Bidder must be responsible for supply, deploy and support the infrastructure.

12 If vendor /OEM does not meet its SLA, IIITD will put the fine of Rs. 2000/- per day for the first seven days and @ Rs.5, 000/- per day from 8th day onwards will be levied.

13 Bidders can seek clarifications, raise technical queries, etc., related to tender by 28-09-2022 via e-mail to **bhawani@iiitd.ac.in**, **adarsh@iiitd.ac.in.** And for financial queries, e-mail to **ajay@iiitd.ac.in.** The reply to clarifications sought or queries raised will be replied to within three days by 01-10-2022 and uploaded on the Institute's website under https://www.iiitd.ac.in.Based on this the bidders may submit bids as prescribed by the due date and time. No clarifications in any other form will be provided.

The following information must accompany the financial Bid:

1	Name, address, and telephone number of the firm/company	
2	Name of the contact person and contact details (mobile/telephone number etc.)	
3	Name of the Bank and full address	
4	Bank Account Number	
5	PAN & GSTIN (Attach self-certified copy)	
6	Valid self-certified copy of authorization from Bidder	
7	Copy of Partnership Deed/ Certificate of registration of the company or any other document evidencing the registration of the Bidder	
8	Number of Years of Experience	
9	Details of DD towards Tender Fee: EMD:	
10	Provide the previous PO's of the same items work executed during the last three years (attested copies of the Orders to be enclosed)	
11	List of service centers, nearest location of the support centre.	
12	Turnover of the Bidder in the financial years: 2018-19 2019-20 2020-21 Please attach CA certified copy of the turnover.	
13	ISO 9000 Certification (please attach certified copy)	

I /We hereby certify that the information furnished above is full and correct to the best of my/our knowledge.

(Signature of the Authorized Signatory)
Name:
Office Seal.

Date:
Place:

TERMS AND CONDITIONS

1. The Financial Bid should be valid for a period of not less than 60 days from the date of opening of Bid.
2. Upon placing of the Purchase Order (PO), the successful Bidder is required to submit a performance bank guarantee (PBG) equivalent to 3% of the PO value within 15 days from the date of PO, failing which the Bidder shall be notified as blacklisted. The PBG will be valid for a period of 60 days beyond the stipulated date for cessation of the contract, which is co-terminus with the warranty period. No interest is payable on the PBG.

3. PBG will be realized by IIIT-D in case of termination of the contract for unsatisfactory performance and/or non-performance of the contract.

4. The Product to be supplied within a period of 6-7 weeks from the date of the Purchase Order by the Institute. If the vendor fails to supply the item as quoted in the Technical & Financial bid, the EMD amount will be forfeited, and the Bidder shall be notified as blacklisted or as deem appropriate by the Institute.

5. The Bidder should have their own test and repair facility with certified engineers.

6. Bids will be opened in the presence of Bidder's representatives, who choose to attend on the specified date and time. Only one representative shall be allowed to attend.

7. Sealed Bid can be sent either by post or by messenger. The responsibility of delivery of Bid lies entirely with the Bidder.

8. 100% payment will be released only on satisfactory installation/services as per the scope of work as certified by the officer in charge of the Institute and after producing the GST invoice. Bidder does not agree to the above payment terms is requested not to submit their Bid.

9. Payment will be paid only if the required SLA as mentioned in the scope of work is met.

10. In the event of a dispute, Director IIIT-Delhi shall be the sole arbitrator, and his decision shall be final and binding on both parties.

11. IIIT-Delhi does not bind itself to accept the lowest or any other offer and reserves the right to accept or reject any or all the offers either in full or in part without assigning any reason.

12. In case the Bidder is not able to execute the work as per terms, EMD/PBG shall be forfeited.

13. Bidder should provide details of its support, certification to this effect from itself. If Bidder fails to meet the SLAs, a fine of 2000/- Rs per day for the first seven days and @ Rs. 5,000/- per day from the 8th day onwards will be levied.

14. The bidder/tenderer shall submit an undertaking on its letter head, duly signed and stamped, that none of the staff, faculty members, relatives, etc. of the Indraprastha Institute of Information Technology-Delhi are related directly or indirectly to any employees, Directors, or Key Managerial Personnel, etc. of the bidder/tenderer. In the event of the IIIT-D coming to know or pointed about the same, the bidder/tenderer undertakes to deposit a sum of Rs.1,00,000/- (Rs. One Lakh only) as a penalty with the Institute. Such bidders/tenderers shall be liable to be blacklisted and announced on the website of IIIT-D.

15. The selected bidder has to sign an agreement with IIITD on a stamp paper after issue of Purchase/Work order. The agreement is attached Annexure ’Y

PROFORMA FOR FINANCIAL BID

S. No.	Details	Qty.	All Inclusive Cost **(Please quote in INR only)**
1	Supply and installation of Next Generation Firewall(As per scope of work)	01	
2	Supply and installation of Next Generation Firewall without subscription(As per scope of work)	01	
	Discount, if any		
	Total Amount Rs.		
	Total Final Cost (in figures) with Installation at IIIT Delhi campus Okhla Phase III, New Delhi. **The Bidder may obtain price in Forex(USD) however the quote in financial Bid should be INR only.** ***If any documents are required for availing custom duty exemption, the IIITD will provide the same. Please quote price accordingly.***		

Please note the price should be quoted for each of the items and should be inclusive of all taxes/charges and installation at IIIT-Delhi.

The discount, if any, should be mentioned herein and nowhere else.

Total Cost (all-inclusive) of quantity mentioned above (in words) at IIIT-Delhi campus:

We accept that the rate quoted above shall remain valid for a period of 60 days from the last date of the tender document, i.e., 60 days from 12th October 2022. It is certified that the rates quoted above are not more than the rates charged from any Central / State Govt. Deptt. / Institution / GeM.

(Signature and Seal of the Bidder)

Annexure Y

ON NON JUDICIAL STAMP PAPER OF RS 100/-

AN AGREEMENT made on day of two thousand Twenty One

BETWEEN

(Hereinafter called the contractor, which expression shall include its proprietor, partners, heirs, executors, administrators, legal representatives, successors and assignees) WITH REGISTERED ADDRESS………………………of the one part

AND

The REGISTRAR Indraprastha Institute of Information Technology Delhi, Okhla Industrial Area Phase III, New Delhi - 110020 (hereinafter called the IIITD, which expression shall include its successors and assignees) of the other part.

Whereas the IIITD had invited Bids <Please write tender name> ; vide its Bid Document No. , which shall be deemed to be a part of this agreement; FOR THE SCOPE OF WORK/SUPPLY

Whereas the contractor submitted its TENDER Bid dated , a copy of the price bid, submitted by the contractor, is annexed hereto as Annexure;

Whereas the IIITD has accepted the Bid submitted by the contractor, on the terms and conditions mentioned in the IIITD's said Bid Document and conveyed its acceptance to the contractor; vide its letter No. dated , AND ANY OTHER CORRESPONDENCE …………………………………which shall be deemed to be a part of this agreement;

Whereas the contractor is agreeable to the terms and conditions mentioned in the IIITD's said Bid document;

Whereas the contractor undertakes to comply with all relevant laws like Contract Labour (Regulation and Abolition) Act, 1970; Employees' State Insurance and Miscellaneous Provisions Act, 1952; Employees' State Insurance Act, 1948; Minimum Wages Act, 1948; Payment of Bonus Act, 1972; Payment of Wages Act, 1936; Income Tax Act; GST Act etc. and to indemnify the IIITD from the contractor’s acts of omission or commission, as regards the compliance with the relevant laws;

Whereas the contractor declares that he/she/it shall own all responsibility for any act of omission or commission, as regards the compliance with the relevant laws;

AND WHEREAS the IIITD is agreeable to make necessary payment to the Contractor, at the rates mentioned in the Annexure annexed hereto and as per the terms and conditions mentioned in the IIITD’s said Bid Document;

In WITNESS whereof Shri (name), (designation), the authorized representative of the contractor, for and on behalf of the contractor, has hereunto set his hand and .... for and on behalf of the IIITD has hereunto set his hand.

(Signature of the authorized representative of the Contractor)

Name and designation of the contractor’s representative

In the presence of

1

2

(Signature of witnesses with full name and full address)

Registrar

for and on behalf of the IIITD

In the presence of

1

2

(Signature of witnesses with full name and full address)