Uluberia College

Tel (+91 33) 2661 0332

Uluberia, Howrah – 711 315

Website: https://www.uluberiacollege.in

Memo No :- **UC/261/2023** Date :- **28.02.2023**

NOTICE INVITING TENDER

Uluberia College invites E-Tender for the work from reputed vendors/authorized partner for supplying the following item (Submission of Bid through online).

1.	E-Tender No.	**WB/DHW/UC/22-23/NIT/E-3 Dated: 28.02.2023**
2.	Name of Work	**Purchase of One Unit of Next Generation Firewall / Cybersecurity Gateway Solution with Three Years License for Uluberia College**
3.	Estimated Cost put to Tender	**NA**
4.	Technical Specification	**Annexure-A**
5.	Earnest Money	Rs. 15000/- Payable to Principal, Uluberia College, Uluberia Howrah 711315
6.	Completion Period	**60 days**
7.	Terms & Conditions	**a) OEM authorization required** **b) The Work order will be awarded to the Lowest (L1) valid Bidder.** **c) The quoted rate should be inclusive of all Govt taxes, loading, unloading, carriage , Power Cord etc complete.** **d) No extra payment to be paid beyond the tendered amount.** **e) The Tender Inviting Authority reserves the right to accept or reject any tender without assuring ant reasons.** **f) Manufacturing Warranty Period:- 3 Years onsite hardware warranty ((No extra payment will be made for any maintenance or up gradation of software package during the guarantee period).** **g) If the Agency fails to complete work within the completion time then the Agency will be debarred for applying any tender for 3 years in this college.**

In the event of e-procurement, intending bidder may download the tender documents from the website https://wbtenders.gov.in directly with the help of Digital Signature Certificate. The Earnest Money Deposit (EMD) and documents with **Technical Specification cum Compliance List** in support should be submitted physically to The Office of The Principal, Uluberia College, Uluberia, Howrah-711315.

Both Technical Bid and Financial Bid are to be submitted concurrently duly digitally signed in the website https://wbtenders.gov.in.

Tender documents may be downloaded from website and submission of Technical Bid and Financial Bid will be done as per Date and Time Schedule. The Technical Bid/Proposal is submitted in two parts. The two parts of the proposal are:-

(i) Part – 1 : Technical proposal
a) Folder 1: Prequalification documents.
b) Folder 2: Technical submission by bidder.
(ii) Part – 2 : Financial proposal

Eligibility criteria for participation in the tender:

1. The prospective bidders shall have similar nature of work done and completion certificate from any govt /PSU department which is applicable for eligible in this tender.

N.B: Date of Completion of Project and detail communicational address of client must be indicated in the credential Certificate. [**Non-statutory documents**]

2. Income Tax Return Acknowledgement for the latest Assessment Year, P.T. Deposit Challan for the year 2022-23, Pan Card, GSTIN (Terms and Conditions apply), Current Trade License.

[**Non-statutory documents**]

3. Registered Partnership Deed for Partnership Firm is to be submitted. The Company shall furnish the Article of Association and Memorandum. Where an individual person holds a digital certificate in his own name duly issued to him against the company or the Firm of which he happens to be a Director or Partner, such individual person shall, while uploading any tender for and on behalf of such Company or Firm, invariably upload a copy of Registered Power of Attorney Showing clear authorization in his favour, by the rest of the Directors of such Company or the Partners of such Firm, to upload such tender. [**Non-statutory documents**]

A prospective bidder shall be allowed to participate in a particular job either in the capacity of individual or as a partner of a firm. If found to have applied severally in a single job, all his applications will be rejected for that job, without assigning any reason thereof.

Date and Time schedule :

SL. No	Particulars Date & Time	Date & Time
1	Date of uploading of N.I.T & other Documents (online) (Publishing Date)	**01-03-2023**
2	Documents download / sale start date (online)	**01-03-2023 AT 2 PM**
3	Bid submission start date (online)	**01-03-2023 AT 2 PM**
4	Bid submission closing date (online)	**14-03-2023 AT 6.55 PM**
5	Date & time of submission of supporting document for Earnest Money Deposit and other Technical Document to The office of Principal, Uluberia College, Uluberia, Howrah, West Bengal-711315	**15.03.2023 From 11am to 3.00 pm**
6	Bid opening date for Technical proposal (Folder 1: Prequalification documents and Folder 2: Technical submission by bidder) (Online)	**17-03-2023 at 1.00 PM**
7	Date of uploading list for Qualified Bidder in Technical Proposal	**After evaluation of Technical Proposal**
8	Date for opening of Financial Proposal (Online)	**To be notified later on.**

SECTION – A INSTRUCTION TO BIDDERS

A. General Guidance for e-Tendering:

A.1. Registration of Contractor:

Any contractor willing to take part in the process of e-Tendering will have to be enrolled & registered with the Government e-procurement System, through logging on the https://wbtenders.gov.in The contractor is to click on the link for e-Tendering site as given on the web portal.

A.2. Digital Signature certificate (DSC) :

Each contractor is required to obtain a Class-II or Class-III Digital Signature Certificate (DSC) for submission of tenders from the approved service provider of the National Informatics Centre (NIC) on payment of requisite amount. Details are available at the web site stated in Clause A.1. above DSC is given as a USB e-Token.

A.3. The contractor can search and download N.I.T., Tender Document(s) and addenda & Corrigenda (if any) electronically from computer once he logs on to the website mentioned in Clause A.1. Using the Digital Signature Certificate. This is the only mode of collection of Tender Documents.

A.4 Participation in more than one work:

A prospective bidder shall be allowed to participate in the job either in the capacity of individual or as a partner of a firm. If found to have applied severally in a single job all his applications will be rejected for that job. A prospective bidder (including his participation in partnership) shall be allowed to participate in single building or repairing work as mentioned in the list of schemes.

A.5. Submission of Tenders:

Tenders are to be submitted through online to the website stated in Clause A.1. in two folders at a time for each work , one is Technical Proposal & the other is Financial Proposal before the prescribed date & time using the Digital Signature Certificate(DSC) Virus free scanned copy of the documents are to be uploaded duly Digital Signed. The documents will get encrypted (transformed into non readable formats).

A.5.1. Technical Proposal:

The Technical proposal should contain scanned copies of the following in two covers (folders).

A5.1.1: Technical Cover containing the following documents:

i) NIT (Download from the e-Tender)

ii) D.D. / Pay Order Payable to Principal, Uluberia College, Uluberia Howrah-711315, for Earnest Money (EMD) as prescribed in the N.I.T against the work and any other Documents like **Technical Specification cum Compliance List etc.**

A5.1.2: Financial Cover containing the following documents:

i) BOQ

A5.1.3: Non statutory Cover containing the following documents

i) Professional Tax (PT) deposit receipt challan for the financial year 2022-23, PAN Card, ITR Acknowledgement for the Assessment year 2021-22, GSTIN with last Acknowledgement.

ii) Registration Certificate under Company Act. Trade License as the case may be.

iii) Registered Deed of partnership Firm/Article of Association & Memorandum

iv) Power of Attorney (For Partnership Firm/Private Limited Company).

v) Technical Specification cum Compliance List

The above stated Non-statutory/Technical Documents should be arranged in the following manner

Click the check boxes beside the necessary documents in the My Document list and then click the tab "Submit Non Statutory Documents' to send the selected documents to Non-Statutory folder. Next Click the tab "Click to Encrypt and upload" and then click the "Technical" Folder to upload the Technical Documents.

Sl.No	Category Name	Sub-Category Description	Detail(s)
A	Certificate(s)	Certificate(s)	1. GST & Service Tax Registration Certificate & Acknowledgement. 2. PAN 3. P Tax(Challan)(2022-23) 4. Latest IT Receipt. 5. IT-Saral for A.Y. 2022-23
B	Company Detail(s)	Company Detail-1	1. Proprietorship Firm (Trade License) Section – B From-II[Structure & Org]. 2. Partnership Firm (Partnership Deed, Trade License) 3. Ltd. Company(Incorporation Certificate, Trade License) 4. Power of Attorney, Memorandum of Association and Articles of Association of the Company.
C	Credential	Credential-1	1. Similar nature of work done and completion certificate from any govt /PSU department which is applicable for eligible in this tender.

A.5.2 Tender Evaluation Committee (TEC)

A.5.2.1 Tender Committee members will act as Evaluation Committee for selection of technically qualified contractors.

A.5.2.2 Opening of Technical Proposal: Technical proposal will be opened by the Tender Committee member/s electronically from the Website using their Digital Signature Certificate (DSC).

A.5.2.3: Intending tenderers may remain present if they so desire.

A.5.2.4: Cover(folder) for Statutory Documents will be opened first and if found in order, cover(folder) for Non-Statutory Documents will be opened.

A.5.2.5: Decrypted (transformed into readable formats) documents of the non-statutory cover will be downloaded & handed over to the Tender Evaluation Committee.

A.5.2.6: Pursuant to scrutiny & decision of the Tender Evaluation Committee the summary list of eligible tenderers & the serial number of work for which their proposal will be considered will be uploaded in the web portals.

A.5.2.7: During evaluation the committee may summon of the tenderer& seek clarification/information or original hard copy of any of the documents already submitted & if these are not produced within the stipulated time frame, their proposals will be liable for rejection.

A.5.3**: Financial Proposal:**

A.5.3.1: The financial proposal should contain the following documents in one cover (folder) i.e. Bill of Quantities(BOQ). The contractor is to quote the rate online through computer in the space marked for quoting rate in the BOQ..

A.5.3.2: Only downloaded copies of the above documents are to be uploaded after Virus scan & Digitally signed by the contractor.

A.6. Financial capacity of a bidder will be judged on the basis of working Financial Statement. If an applicant feels that his/their Working Capital from own resource may be insufficient, he/they may include with the application letter of guarantee issued by a first class Bank to supplement the applicant. This letter of guarantee should be addressed to the Tender Inviting/Accepting Authority and should guarantee duly specifying the name of the project that in case of contract is awarded to the Bidder, the Bidder will be provided with a revolving line of credit. Such revolving line of credit should be maintained until the works are taken over by the Engineer-in-charge/Employer.

The audited Balance sheet for the last year, net worth, bid capacity, etc. are to be submitted which must demonstrate the soundness of Bidder's financial position, showing long term profitability including an estimated financial projection of the next two years.

A.7: Penalty for suppression/distortion of facts:

If any tenderer fails to produce the original hard copies of the documents (especially Completion Certificates and Audited Balance Sheets) Or any other documents on demand of the Tender Evaluation. Committee within a specified time frame or if any deviation is detected in the hard copies from the uploaded soft copies, it may be treated as submission of false documents by the tenderer and action may be referred to the appropriate authority for prosecution as per relevant IT Act.

A.8: Rejection of Bid:

Employer Reserves the right to accept or reject any Bid and to cancel the Biding processes and reject all Bids at any time prior to the award of contract without thereby incurring any liability to the affected Bidder or Bidders or any obligation to inform the affected Bidder or Bidders of the ground for Employer's action.

A.9: Award of Contract:

The Bidder whose Bid has been accepted will be notified by the Tender Inviting & Accepting Authority through acceptance letter/Letter of Acceptance.

The notification of award will constitute the formation of the Contract:

The Agreement in West Bengal From No. 2911(ii) will incorporate all agreements between the Tender Accepting Authority and the successful bidder. All the tender documents including N.I.T & B.O.Q will be the part of the contract documents. After receipt of Letter of Acceptance, the successful bidder shall have to submit

requisite copies of contract documents along with requisite of the concerned work within time limit to be set in the letter of acceptance.

To be submitted in Non-Judicial Stamp Paper, and it should be notarized

DECLARATION TO BE GIVEN ALL BIDDERS PARTICIPATING IN TENDER

This is to declare that, as on date of submission of this tender, we have not been banned/Put on hold or delisted by any government or quasi Government agencies or PSUs.

Sign & seal of the Bidder

Technical Specification cum Compliance List

Annexure A

NGFW Technical Specifications (Sophos, Palo Alto, CheckPoint Preferable)	Compliance (Y/N)
Hardware Architecture & Performance	
The appliance based security platform should be capable of providing firewall, application visibility, Web Protection and IPS functionality in a single appliance	
The appliance hardware should be a multicore CPU architecture with a hardened 64 bit operating system to support minimum 12 GB memory. Should have additional NPU with 8 core preocessor & 4 GB RAM for hardware accelaration .	
Should support minimum 240 GB SSD for logs & reports	
The appliance should support atleast 8 * 1G ports 2 * 1G SFP ports & 2*10G SFP+ ports from day 1 . The appliance should have option to support additional 4 * 10G ports in future.	
Should support atleast 32 Gbps Firewall throughput & 8 Gbps of NGFW throughput	
Proposed appliance should support atleast 12 million concurrent sessions or more	
Firewall should support atleast 150K connections per second or more	
Solution should have 15 Gbps of IPSec VPN throughput	
Firewall Should support atleast 2 Gbps of Threat Protection Throught (Measured with Firewall, IPS, Application Control, and Malware prevention enabled)	
Solution should have 2.2 Gbps SSL/TLS inspection throughput	
Industry Certification	
Solution should have FIPS & ICSA certified	
Solution should provide make in india certificate with minimum 65% local content	
Solution should have TEC certificate recommended by MeitY	
Solution should be NSS lab certified with minimum 93% exploit block rate	
General Management	
Purpose-built, streamlined user interface and firewall rule management for large rule sets with grouping with at-a-glance rule feature and enforcement indicators	
Two-factor authentication (One-time-password) support for administrator access, user portal, IPSec and SSL VPN	
Firewall should support TLS 1.3 inspection of encrypted traffic	
Firewall should support Xstream FastPath technology for application acceleration	
Firewall should be ready for Xtended Detection & Response and Synchronized SDWAN	
Solution should provide Managed Detection & Response capability and must have single console to manage Endpoint, Server, email , mobile protection & Firewall security appliances.	
High Availability (HA) support clustering two devices in active-active or active-passive mode.	
Full command-line-interface (CLI) accessible from GUI	
Automated firmware update notification with easy automated update process and roll-back features	
Reusable system object definitions for networks, services, hosts, time periods, users and groups, clients and servers	

Jumbo Frame Support , Self-service user portal	
SNMPv3 and Netflow support , API for 3rd party integration	
Backup and restore configurations: locally, via FTP or email; on-demand, daily, weekly or monthly	
Firewall, Networking & Routing	
Stateful deep packet inspection firewall	
Network Flow FastPath acceleration for trusted traffic	
User, group, time, or network based policies	
Access time polices per user/group	
Enforce policy across zones, networks, or by service type	
Zone isolation and zone-based policy support	
Default zones for LAN, WAN, DMZ, LOCAL, VPN and WiFi	
Custom zones on LAN or DMZ	
Customizable NAT policies with IP masquerading and full object support to redirect or forward multiple services in a single rule	
Flood protection: DoS, DDoS and portscan blocking Country blocking by geo-IP	
Routing: static, multicast (PIM-SM), and dynamic (RIP, BGP, OSPF)	
Protocol independent multicast routing with IGMP snooping	
Bridging with STP support and ARP broadcast forwarding	
VLAN DHCP support and tagging,VLAN bridge support	
WAN link balancing: multiple Internet connections, auto-link health check, automatic failover, automatic and weighted balancing, and granular multipath rules	
Full configuration of DNS, DHCP and NTP, 802.3ad interface link aggregation	
IPv6 tunnelling support including 6in4, 6to4, 4in6, and IPv6 rapid deployment through IPSec	
Flexible network or user based traffic shaping (QoS) (enhanced Web and App traffic shaping options included with the Web Protection subscription)	
Set user-based traffic quotas on upload/download or total traffic and cyclical or non-cyclical	
Authentication	
Synchronized User ID utilizes Synchronized Security to share currently logged in Active Directory user ID between Sophos endpoints and the firewall without an agent on the AD server or client	
Authentication via: Active Directory, eDirectory, RADIUS, LDAP and TACACS+	
Server authentication agents for Active Directory SSO, STAS, SATC	
Single sign-on: Active directory, eDirectory, RADIUS Accounting	
Client authentication agents for Windows, Mac OS X, Linux 32/64	
Browser SSO authentication: Transparent, proxy authentication (NTLM) and Kerberos	
Browser Captive Portal	

Authentication certificates for iOS and Android	
Authentication services for IPSec, SSL, L2TP, PPTP	
Google Chromebook authentication support for environments with Active Directory and Google G Suite	
Next Gen VPN Support	
Site-to-site VPN: SSL, IPSec, 256- bit AES/3DES, PFS, RSA, X.509 certificates, pre-shared key	
L2TP and PPTP,Route-based VPN	
Remote access: SSL, IPsec, iPhone/iPad/ Cisco/Andriod VPN client support,IKEv2 Support	
SSL client for Windows and configuration download via user portal	
Encrypted HTML5 self-service portal with support for RDP, HTTP, HTTPS, SSH, Telnet, and VNC	
Authentication: Pre-Shared Key (PSK), PKI (X.509), Token and XAUTH	
Enables Synchronized Security and Security Heartbeat for remote connected users	
Unilimited IPSec & SSL client with unlimited 2factor mobile (android & IOS) authenticator license	
Single client support for IPSec & SSL remote VPN	
Mac and Windows Support	
Intrusion Prevention (IPS)	
High-performance, next-gen IPS deep packet inspection engine with selective IPS patterns that can be applied on a firewall rule basis for maximum performance and protection	
Minimum 5000 of signatures,Support for custom IPS signatures	
Advanced Threat Protection (detect and block network traffic attempting to contact command and control servers using multi-layered DNS, AFC, and firewall)	
Security Heartbeat instantly identifies compromised endpoints including the host, user, process, incident count, and time of compromise	
Security Heartbeat policies can limit access to network resources or completely isolate compromised systems until they are cleaned	
Lateral Movement Protection further isolates compromised systems by having healthy -managed endpoints reject all traffic from unhealthy endpoints preventing the movement of threats even on the same broadcast domain	
Web Protection and Control	
Fully transparent proxy for anti-malware and web-filtering	
Enhanced Advanced Threat Protection	
URL Filter database with millions of sites across 92 categories backed by OEMLabs	
Surfing quota time policies per user/group ,Access time polices per user/group	
Malware scanning: block all forms of viruses, web malware, trojans and spyware on HTTP/S, FTP and web-based email	
Advanced web malware protection with JavaScript emulation	
Live Protection real-time in-the-cloud lookups for the latest threat intelligence	
Second independent malware detection engine for dual-scanning	

HTTP and HTTPS scanning on a per user or network policy basis with customizable rules and exceptions	
File type filtering by mime-type, extension and active content types (e.g. Activex, applets, cookies, etc.)	
YouTube for Schools enforcement per policy (user/group)	
SafeSearch enforcement (DNS-based) for major search engines per policy (user/group)	
Web keyword monitoring and enforcement to log, report or block web content matching keyword lists with the option to upload customs lists	
Block Potentially Unwanted Applications (PUAs)	
Web policy override option for teachers or staff to temporarily allow access to blocked sites or categories that are fully customizable and manageable by select users	
User/Group policy enforcement on Google Chromebooks	
Control Center widget displays amount of data uploaded and downloaded to cloud applications categorized as new, sanctioned, unsanctioned or tolerated	
Application Protection and Control	
Synchronized App Control to automatically, identify, classify, and control all unknown Windows and Mac applications on the network by sharing information between Sophos-managed endpoints and the firewall	
Signature-based application control with patterns for thousands of applications	
Cloud Application Visibility and Control to discover Shadow IT	
App Control Smart Filters that enable dynamic policies which automatically update as new patterns are added	
Micro app discovery and control	
Application control based on category, characteristics (e.g., bandwidth and productivity consuming), technology (e.g. P2P), and risk level	
Per-user or network rule application control policy enforcement	
Web Application Firewall Protection	
Reverse proxy,URL hardening engine with deep-linking and directory traversal prevention	
Form hardening engine SQL injection protection Cross-site scripting protection HTTPS (TLS/SSL) encryption offloading Cookie signing with digital signatures Path-based routing Outlook anywhere protocol support Reverse authentication (offloading) for form-based and basic authentication for server access	
Integrated load balancer spreads visitors across multiple servers	
Options to change Web Application Firewall performance parameters Scan size limit option Allow/Block IP ranges Wildcard support for server paths and domains Automatically append a prefix/suffix for authentication	
36 months License Includes :	
Network Protection Subscriptions (IPS,HTML5, ATP, Anti-malware),	
Web Protection Subscriptions (URL, AppCtrl, Web/App Traffic Shaping),	

Zero Day Protection & SDWAN synchronization management console with 100 device license	
24 X 7 hardware & warranty support from OEM	
The firewall should be compatible with zero day protection and collaborating with extended detection and response with end points	
Do you have OEM authorization