SNDB/COK/ADMIN/TD/1194/2021
COPY NO: _______________

Sindh Bank Limited

Tender Document
Supply and Installation of Web Application Firewall
(WAF-2)

Table of Contents

DEFINITIOS

"Bid" means a tender, or an offer by a person, consultant, firm, company or an organization expressing willingness to undertake a specified task at a price, in response to an invitation by SNDB.

"Bidding Documents" means the documents notified by the Authority for preparation of bids in uniform manner.

"Bidding Process" means the procurement procedure under which sealed bids are invited, received, opened, examined and evaluated for the purpose of awarding a contract;

"Blacklisting" means barring (or debarring) a bidder, contractor, consultant or supplier from participating in any future procurement proceedings by SNDB.

"Calendar Days" means days including all holidays;

"Conflict of Interest" means -

(i) where a contractor, supplier or consultant provides, or could provide, or could be perceived as providing biased professional advice to SNDB to obtain an undue benefit for himself or those affiliated with him;

(ii) receiving or giving any remuneration directly or indirectly in connection with the assignment except as provided in the contract;

(iii) any engagement in consulting or other procurement activities of a contractor, consultant or service provider that conflicts with his role or relationship with the SNDB under the contract;

(iv) where an official of the SNDB engaged in the procurement process has a financial or economic interest in the outcome of the process of procurement, in a direct or an indirect manner;

"Consultant" means a professional who can study, design, organize, evaluate and manage projects or assess, evaluate and provide specialist advice or give technical assistance for making or drafting policies, institutional reforms and includes private entities, consulting firms, legal advisors, engineering firms, construction managers, management firms, procurement agents, inspection agents, auditors, international and multinational organizations, investment and merchant banks, universities, research institutions, government agencies, nongovernmental organizations, and individuals;

"Consulting Services" means services of an advisory and intellectual nature provided by consultants using their professional skills to study, design, organize, and manage projects, encompassing multiple activities and disciplines, including the crafting of sector policies and institutional reforms, specialist advice, legal advice and integrated solutions, change management and financial advisory services, planning and engineering studies, and architectural design services, supervision, social and environmental assessments, technical assistance, and programme implementation**;**

"Contract" means an agreement enforceable by law and includes General and Special Conditions, Specifications, Drawings and Bill of Quantities;

“Contractor” means a person, firm, company or organization that undertakes to execute works including services related thereto, other than consulting services, incidental to or required for the contract being undertaken for the works;

“Corrupt and Fraudulent Practices” means either one or any combination of the practices given below;

“**Coercive Practice**” means any impairing or harming, or threatening to impair or harm, directly or indirectly, any party or the property of the party to influence the actions of a party to achieve a wrongful gain or to cause a wrongful loss to another party;

“**Collusive Practice**” means any arrangement between two or more parties to the procurement process or contract execution, designed to achieve with or without the knowledge of the SNDB to establish prices at artificial, non-competitive levels for any wrongful gain;

“Corrupt Practice” means the offering, giving, receiving or soliciting, directly or indirectly, of anything of value to influence the acts of another party for wrongful gain;

“**Fraudulent Practice”** means any act or omission, including a misrepresentation, that knowingly or recklessly misleads, or attempts to mislead, a party to obtain a financial or other benefit or to avoid an obligation;

“Obstructive Practice” means harming or threatening to harm, directly or indirectly, persons or their property to influence their participation in a procurement process, or affect the execution of a contract or deliberately destroying, falsifying, altering or concealing of evidence material to the investigation or making false statements before investigators in order to materially impede an investigation into allegations of a corrupt, fraudulent, coercive or collusive practice; or threatening, harassing or intimidating any party to prevent it from disclosing its knowledge of matters relevant to the investigation or from pursuing the investigation, or acts intended to materially impede the exercise of inspection and audit rights provided for under the Rules.

“Emergency” means natural calamities, disasters, accidents, war and breakdown of operational equipment, plant, machinery or engineering infrastructures, which may give rise to abnormal situation requiring prompt and immediate action to limit or avoid damage to person(s), property or the environment;

“Government” means the Government of Sindh;

“Head of the Department” means the administrative head of the department or the organization;

“Lowest Evaluated Bid” means a bid most closely conforming to evaluation criteria and other conditions specified in the bidding document, having lowest evaluated cost.

“Lowest Submitted Price” means the lowest price quoted in a bid, which is otherwise not substantially responsive;

“Notice Inviting Tender” means the notice issued by a SNDB through publication in the newspapers or through electronic means for the purpose of inviting bids, or applications for pre-qualifications, or expression of interests, which may include Tender Notice, Invitation for Bids, Notice for Pre-qualifications or Request for Expression of Interests;

“Open Competitive Bidding” means a fair and transparent specified procedure defined under these Rules, advertised in the prescribed manner, leading to the award of a contract whereby all interested persons, firms, companies or organizations may bid for the contract and includes both National and International Competitive Biddings;

“**SNDB**” means the Sindh Bank Limited;

“Services” includes physical, maintenance, professional, intellectual, consultancy or advisory services but does not include appointment of an individual to a post or office, advertisement, arbitration, conciliation or mediation services, services of an advocate in a court case or any other services specifically excluded under the rules;

“Supplier” means a person, firm, company or an organization that undertakes to supply goods and services related thereto, other than consulting services, required for the contract;

“Value for Money” means best returns for each rupee spent in terms of quality, timeliness, reliability, after sales service, up-grade ability, price, source, and the combination of whole-life cost and quality to meet SNDB’s requirements.

1 INVITATION ON FOR BIDS (IFB)

Sindh Bank Limited (SNDB) invites proposal from reputed vendors for Supply and Installation of Web Application Firewalls (WAF - 2). Details of the specifications to be provided are given in the scope of work/technical specifications in Section [3] hereto.

Bidders will be selected under procedure described in this tender document in accordance with the Sindh Public Procurement Rules 2010 (Amended 2019) and instructions to bidders ITB given under SPPRA bidding document for national competitive bidding Pakistan – procurement of goods, which can be found at www.pprasindh.gov.pk/. For the purposes of this document, any reference to the term “Act” shall mean a reference to the Sindh Public Procurement Act 2009 and any reference to the Rules shall mean a reference to the Sindh Public Procurement Rules 2010.(Amended 2019)

This TENDER Documents includes the following Sections

- Instructions to Bidders (ITB)
- Eligibility Criteria
- Scope of Work / Technical Proposal
- Financial Proposal
- Conditions of Contract

Proposals must be submitted at the below mentioned address;

Yours sincerely,

Head of Administration
SINDH BANK LIMITED
HEAD OFFICE
Basement-2 Floor, Federation House,
Abdullah Shah Ghazi Road,
Clifton,
Karachi 75600

2 INSTRUCTION TO BIDDERS (ITB)

For All legal purpose, all clauses of instructions to bidders (ITB) hoisted by SPPRA on their website www.sppra.org will be taken as part and parcel of this tender document and the agreement thereof. Accordingly the bidders are advised in their own interest to go through the same meticulously as ignorance of the said ITB will not be taken as excuse to waive off any plenty or legal proceedings.

However, few important clauses of the above mentioned ITB are appended below for the guidance/perusal of the bidders.

2.1 Correspondence Address

The contact number and the correspondence address for submitting the proposals are as follow:

Head of Administration
SINDH BANK LIMITED
HEAD OFFICE
Basement-2 Floor, Federation House,
Abdullah Shah Ghazi Road,
Clifton,
Karachi 75600

2.2 Eligible Bidders

All the bidders duly incorporated and based in Pakistan governed by rules, laws and statutes of Government of Pakistan and Government of Sindh shall be eligible. [SPPRA Rule 29]

2.3 Corrupt Practice

1. SNDB requires that Bidders / Suppliers / Contractors, observe the highest standard of ethics during the procurement and execution of contract and refrain from undertaking or participating in any corrupt or fraudulent practices. [SPPRA Rule 2 (q – iii, iv)]

2. SNDB will reject a proposal for award, if it determines that the Bidder recommended for award was engaged in any corrupt or has been blacklisted under the Sindh Public Procurement Rules 2010 (Amended 2019), in competing for the contract in question.

3. Any false information or misstatement on the part of the vendor will lead to disqualification/ blacklisting/ legal proceeding regardless of the price or quality of the product.

2.4 Preparation of Bids

2.4.1 Bidding Process

This is the Single Stage – One Envelope Procedure; the bid shall comprise a single package containing **TECHINCAL**, **ELIGIBILITY CRITERIA & FINANCIAL PROPSOAL** (duly filled in all respect). [SPPRA Rule 46 (1-a&b)]

2.4.2 Cost of Bidding

The bidder shall bear all costs associated with the preparation and submission of its bid and SNDB will in no case be responsible or liable for those costs, regardless of the conduct or outcome of the bidding process.

2.4.3 Language of Bid

The bid prepared by the bidders as well as all correspondence and documents exchanged by the bidder and SNDB must be written in English. [SPPRA Rule 6 (1)]

2.4.4 Technical Proposal

Bidders are required to submit the Technical Proposal alongwith the specifications asked in the section- scope of work with brief description of the bidder's organization outlining their recent experience, professional staff who participates during the assignment, the technical approach, sample templates/prototypes of deliverables, methodology, work plan and organization, including workable suggestions that could improve the quality and effectiveness of the assignment. The Technical proposal shall be duly signed by the authorized representative of the Bidder not including any financial information otherwise it will be declared as non-responsive.

2.4.5 Financial Proposal

The Financial Proposal shall be prepared using the standard form attached, duly signed by the authorized representative of the Bidder. It should list all costs inclusive taxes associated with the assignment including remuneration for staff, and reimbursable expenses and such other information as may be specifically requested by SNDB. Adding of any condition on the said format will not be taken in to consideration.

2.4.6 Bid Currencies

For the purpose of comparison of bids quoted in different currencies, price shall be converted in PAK RUPEE (PKR). The rate of exchange shall be the selling rate prevailing seven working days before the date of opening of the bids. [SPPRA Rule 42 (2)]

2.4.7 Bid Security

The SNDB shall require the bidders to furnish the Earnest Money @ 5% of Bidding Cost or Irrevocable Bank Guarantee acceptable to the bank, which shall remain valid for a period of twenty eight (28) days beyond the validity period for bids, in order to provide the SNDB reasonable time to act, if the security is to be called. [SPPRA Rule 37(1)]

Bid Security should be attached with Financial Proposal. Bidders are also required to submit affidavit that the Bid Security has been attached with the Financial Proposal.

Any Bid not accompanied by an acceptable Bid Security shall be rejected by the SNDB as non – responsive.

Bid security shall be released to the unsuccessful bidders once the contract will be signed with the successful bidder or the validity period has expired. [SPPRA Rule 37(2)]

The bid security shall be forfeited:

- If a Bidder withdraws its bid during the period of its validity specified by the Bidder on the Bid Form; or
- In the case of a successful Bidder, if the Bidder fails to;
  - Sign the contract in accordance with ITB Section [2.7.4]; or
  - Furnish performance security in accordance with ITB Section [2.7.5].

2.4.8 Bid Validity

Bids shall remain valid for a period of ninety (90) days, after the date of bid opening prescribed by SNDB; [SPPRA Rule 38 (1)]

Whenever an extension of bid validity period is requested, a bidder shall have the right to refuse to grant such an extension and withdraw his bid and bid security shall be returned forthwith; and [SPPRA Rule 38 (6)]

Bidders who agree to extension of the bid validity period shall also extend validity of the bid security for the agreed extended period of the bid validity. [SPPRA Rule 38 (7-a)]

2.5 Submission of Bids

2.5.1 Sealing and Marking of Bids

This is the Single Stage – One Envelope Procedure; the bid shall comprise a single package containing **TECHINCAL, ELIGIBILITY CRITERIA & FINANCIAL PROPOSAL** (duly filled in all respect) [SPPRA Rule 46 (1-a & b)]

2.5.2 Response Time

Bidders are required to submit their Bids within fifteen (15) calendar days from the date of publication of Notice Inviting Tender as per National Competitive Bidding. Bids must be received by SNDB at the address specified under ITB Section [2.1] within office hours. [SPPRA Rule 18 (2)]

2.5.3 Extension of Time Period for Submission of Bids

SNDB may extend the deadline for submission of bids only, if one or all of the following conditions exist;

- Fewer than three bids have been submitted and SNDB is unanimous in its view that wider competition can be ensured by extending the deadline. In such case, the bids submitted shall be returned to the Bidders un-opened; [SPPRA Rule 22 (1)]

- If the SNDB is convinced that such extraordinary circumstances have arisen owing to law and order situation or a natural calamity that the deadline should be extended. [SPPRA Rule 22 (2)]

2.5.4 Clarification of Bidding Documents

An interested bidder, who has obtained bidding documents, may request for clarification of contents of the bidding document in writing, and SNDB shall respond to such queries in writing within three calendar days, provided they are received at least five (5) calendar days prior to the date of opening of bid. [SPPRA Rule 23 (1)]

It should be noted that any clarification to any query by a bidder shall also be communicated to all parties, who have obtained biding documents.

2.5.5 Late Bids

Any bid received by SNDB after the deadline for submission of bids prescribed by SNDB pursuant to ITB Section [2.5.2] will be rejected and returned unopened to the Bidder. [SPPRA Rule 24 (1)] .The rejection of bids received after the deadline for submission shall apply regardless of any reason whatsoever for such delayed receipt.

2.5.6 Withdrawal of Bids

The Bidder may withdraw its Technical Proposal and Financial Proposal after it has been submitted by sending a written Withdrawal Notice, duly signed by the Bidder and/or by an authorized representative, and shall include a copy of the authorization. Provided that, written notice of Withdrawal, shall be received by SNDB prior to the opening of bids.

No bid shall be withdrawn in the interval between the opening of Bids and the expiration of the period of Bid validity specified in ITB section [2.4.8].

2.5.7 Cancellation of Bidding Process

1. SNDB may cancel the bidding process at any time prior to the acceptance of a bid or proposal; [SPPRA Rule 25 (1)]

2. SNDB shall incur no liability towards the bidders, solely by virtue of its invoking sub-rule (2.5.7 - 1); [SPPRA Rule 25 (2)]

3. Intimation of the cancellation of bidding process shall be given promptly to all bidders and bid security shall be returned along with such intimation; [SPPRA Rule 25 (3)]

4. SNDB shall, upon request by any of the bidders, communicate to such bidder, grounds for the cancellation of bidding process, but is not required to justify such grounds. [SPPRA Rule 25 (4)]

2.5.8 Mechanism for Redressal of Grievances

SNDB has a Committee for Complaint Redressal to address the complaints of bidder that may occur during the procurement proceedings. [SPPRA Rule 31 (1)]

Any bidder being aggrieved by any act or decision of the SNDB after the issuance of notice inviting tender may lodge a written complaint [SPPRA Rule 31(3)].

The complaint redressal committee upon receiving a complaint from an aggrieved bidder may, if satisfied; [SPPRA Rule 31(4)]

1. prohibit the procurement committee from acting or deciding in a manner, inconsistent with these rules and regulations; [SPPRA Rule 31(4-a)]

2. annul in whole or in part, any unauthorized act or decision of the procurement committee; [SPPRA Rule 31(4-b)] and

3. [recommend to the Head of Department that the case be declared a mis- procurement if material violation of Act, Rules Regulations, Orders, Instructions or any other law relating to public procurement, has been established; [SPPRA Rule 31(4-bb)] and]

4. reverse any decision of the procurement committee or substitute its own decision for such a decision;

   Provided that the complaint redressal committee shall not make any decision to award the contract. [SPPRA Rule 31(4-c)]

[Complaint redressal Committee of (SNDB) shall announce its decision within seven (7) days. and intimate the same to the Bidder and the Authority within three (3) working days by SNDB. If the committee stand transferred to the Review Committee which shall dispose of the complaint in accordance with the procedure laid down in Rule 32,] [if the aggrieved bidder files the review appeal within ten (10) days of such transfer] [SPPRA Rule 31(5)]

SNDB shall award the contract only after the decision of the complaint redressal committee [SPPRA Rule 31 (6)]

Mere fact of lodging of a complaint shall not warrant suspension of the procurement proceedings. [SPPRA Rule 31(7)].

Provided that in case of failure of the complaint Redressal Committee to decide the complaint; SNDB shall not award the contract. [until the expiry of appeal period or the final adjudication by the Review Committee]

IMPORTANT

In addition to above it may be added that no complaint will be entertained unless it is:-

a) Forwarded on company's original letter head, complete address, NTN of the company and CNIC of the complainant.
b) Incriminating evidence of the complaints.

2.5.9 Appeal to Review Committee

A bidder not satisfied with decision of the SNDB Complaints Redressal Committee may lodge an appeal to the Review Committee; [within ten (10) days of announcement of the decision]. provided that he has not withdrawn the bid security, if any, deposited by him. [SPPRA Rule 32 (1)].

The bidder shall submit the following documents to the Review Committee: [SPPRA Rule 32 (5)].

(a) A letter stating his wish to appeal to the Review Committee and nature of complaint; [SPPRA Rule 32 (5-a)].

(b) A copy of the complaint earlier submitted to the complaint Redressal committee of the department and all supporting documents; [SPPRA Rule 32 (5-b)].

(c) Copy of the decision of Procuring Agency / Complaint Redressal Committee. [if any] [SPPRA Rule 32 (5-c)].

On receipt of appeal, [along with all requisite information & documents] the Chairperson shall convene a meeting of the Review Committee within seven working days; [SPPRA Rule 32 (6)].

It shall be mandatory for the appellant and the Head of SNDB or his nominee not below the rank of BS-19 to appear before the Review Committee as and when called and produce documents, if required; [SPPRA Rule 32 (8)].

In case the appellant fails to appear twice despite the service of notice of appearance, the appeal may be decided ex-parte [SPPRA Rule 32 (9)].

The Review Committee shall hear the parties and announce its decision within ten working days of submission of appeal;[However, in case of delay, reasons thereof shall be recorded in writing] [SPPRA Rule 32 (10)].

The decision of Review Committee shall be final and binding upon the SNDB. After the decision has been announced, the appeal and decision thereof shall be hoisted by the Authority on its website; [SPPRA Rule 32 (11)].

2.5.10 Matters not subject to Appeal or Review

The following actions of the SNDB shall not be subject to the appeal or review: [SPPRA Rule 33]

- Selection method adopted by the SNDB; [SPPRA Rule 33 (1)]
- Decision by the SNDB under ITB section [2.5.7]. [SPPRA Rule 33 (2)

2.6 Opening and Evaluation of Bids

2.6.1 Opening of Bids by SNDB

The opening of bids shall be as per the procedure set down in Section 2.4.1 dealing with Bidding Process.

2.6.2 Clarification of Bids

No Bidder shall be allowed to alter or modify his bids after the expiry of deadline for the receipt of the bids; provided, SNDB may at its discretion, ask a Bidder for clarifications needed to evaluate the bids but shall not permit any bidder to change the substance or price of the bid. Any request for clarification in the bid made by the SNDB, shall invariably be in wiring. The response to such request shall also be in writing. [SPPRA Rule 43]

2.6.3 Preliminary Examination

SNDB will examine the bids to determine whether the bids are complete and the documents have been properly signed and whether the bids are generally in order.

SNDB may waive any minor informality; nonconformity or irregularity in a bid that does not constitute a material deviation, provided such waiver does not prejudice or affect the relative ranking of any Bidder and further provided that such waiver will be at the complete and sole discretion of SNDB.

If a bid is not substantially responsive, it will be rejected by SNDB and may not subsequently be made by the Bidder by correction of the nonconformity.

2.6.4 Supplier Evaluation Criteria

All bids shall be evaluated in accordance with the evaluation criteria. [SPPRA Rule 42 (1)] SNDB will evaluate the bids, which have been determined to be substantially responsive and reject any proposal which does not conform to the specified requirements.

2.6.5 Eligibility Criteria

The prospective Supplier will provide Sindh Bank with One (01) Web application firewall (WAF) that includes the following features.

Bidder/OEM Eligibility Criteria:

The contract will be awarded to the successful Bidder whose bid will be found technically compliant and has offered the lowest cost and emerged as most advantageous bid. Proposed Bidder must qualify following criteria:

1. Bidder must be registered with Income Tax and Sales Tax Department and must appear on Active Taxpayer List of FBR.(YES/NO)
2. Bidder must either be a Manufacturer (OEM) or an authorized Partner of the OEM in Pakistan. (YES/NO)
3. Bidder must have Annual Turnover of at least PKR 15 Million in last Three (03) financial years. Audited Financial reports or Tax Statements to be submitted with the proposal. (YES/NO)
4. Bidder/OEM proposed solution must be deployed in at least Three (03) commercial Banks during last three years other than Sindh Bank. (YES/NO)
5. Bidder must have successfully done Two (02) deployments of Web Application Firewall (WAF) in commercial Banks last three years. (YES/NO)
6. Bidder must have service and support office in at least two (02) major cities of Pakistan including Karachi. (YES/NO)
7. Bidder must not be blacklisted by any government, semi-government, or private organization. (YES/NO)
8. Bidder must submit OEM authorization letter for this specific procurement. (YES/NO)
9. Quoted hardware / Software solution must have end of life beyond five (05) year at the time of submission. (YES/NO)
10. Bidder must be in relevant IT business since last Five (05) years. (YES/NO)
11. Bidder must have at least two professional level certified resource on proposed OEM. (YES/NO)
12. The proposed product must be recognized as a “Leader/Challenger” at-least once in last three (03) years of Gartner Magic Quadrant. (YES/NO)
13. Required quantities of Web application firewall (WAF) is One (01) and will be deployed in Primary data center in High Availability (HA).

ELIGIBILTY CRITERIA NOTE

1. If company not active Tax payer it will consider as a disqualified (Attached Proof as Annexcure-6).
2. There can be a subsequent clarification to this specific tender for which it is advised to keep yourself abreast with the notification being hoisted on Sindh Bank Ltd & SPPRA websites regularly.
3. Attachment of relevant evidence in eligibility criteria is mandatory. In case of non-provision of evidence in any of the requisite, bidder will be disqualified.
4. Bank reserves the right to verify all or any documents from the source, submitted in the bid as per SPPRA rule # 30(1).
5. Bank reserves the right to verify the equipment from the principle at any time to ensure that the supply of equipment is genuine, original, new and that its specification are the same as described in the bid. In case of any fake/refurbished equipment, the company may be subject to legal proceeding as per SPPRA rule # 30(1).
6. Company will be considered disqualified if specification of the WAF quoted does not meet the specification given in the tender document.
7. Company shall supply Goods as per specifications and upon the recommendations of the Technical/Standardized Committee appointed by the Bank within 8 to 10 weeks from the date of receipt of purchase order. In addition to that Rs. 500/- per day will be fined after 10 days and Rs. 1,000/- per day will be fined after 20 days.

MANDATORY

1. GST/Income Tax Registration/Registration With Sindh Revenue Board
2. Attachment of Affidavit (specimen attached as Annexure "H") on stamp paper from the owner of the company.
3. Attachment of Annexure "A" (With Financial Proposal) & Annexure "B" (With Financial Proposal if Bank Guarantee is going to be submitted as Bid Security).
4. Writing of tender reference as given in the NIT on the Envelop, carrying tender document is must or the bank will not be responsible if the documents are not received by the Procurement Committee at the time of opening of bids.
5. The bidders are required to submit bids only in prescribed financial proforma given in Tender Document.
6. The representative present at the time of opening of tender shall be in possession of authority letter on the company's letter head, duly signed by the CEO of the company.
7. The Company must be in I.T. Business for Preferably 05 Years in Pakistan. (Attach documentary proof as Annexure-7)
8. Company must provide a valid & latest Manufacturer Authorization Certificate (MAF) from the Manufacturer/Principal for supply of required equipment.
   (Attach documentary/certificate proof as Annexure-8)

Note: Attachment of relevant evidence is mandatory in eligibility criteria. In case of non-provision of evidence in any of the requisite, bidder will be disqualified.

DISQUALIFICATION

The bidder will be considered disqualified prior to/during technical/financial evaluation process or after award contract if:

1. On black list of SPPRA & Sindh Bank Ltd.
2. Issued with two (2) warning letters/emails by the Sindh Bank Ltd in the past to the bidder for unsatisfactory performances.
3. Not GST/Income Tax Registered/Registration With Sindh Revenue Board
4. Alternate bid is offered.
5. Non - Attachment of Annexure “A” (With Financial Proposal) & Annexure “B” (With Financial Proposal if Bank Guarantee is going to be submitted as Bid Security).
6. The qualified bidder sublets the contract in any form/stage to any other agency.
7. The tender is deposited without Tender Fee.
8. Warranty of supplied items is less than 1 year.
9. If during verification process of the cliental list the response by any of the bank is unsatisfactory on account of previous performance.
10. After supply, if the specification of supplied items is found different with the items produced in front of committee at the time of technical evaluation.
11. In the past, the company agreement has been prematurely been terminated after due qualification in any of the category of the tender.

2.6.6 Discussion Prior to Evaluation

If required, prior to technical evaluation the bidder may seek any clarification in writing on the eligibility criteria.

2.7 Award of Contract

2.7.1 Award Criteria

Subject to ITB Section [2.7.2], SNDB will award the contract to the successful Bidder, whose bid has been determined to be substantially responsive and has been determined to be the lowest evaluated bid, provided further that the Bidder is determined to be qualified to perform the contract satisfactorily.

2.7.2 SNDB’s Right to Accept Any Bid and to reject any or all Bids

SNDB annul the bidding process and reject all Bids at any time prior to Contract award, without thereby incurring any liability to the Bidder(s).

2.7.3 Notification of Award

Prior to the expiration of the period of bid validity, SNDB will notify the successful Bidder in writing by letter or by facsimile, to be confirmed in writing by letter, that his/her bid has been accepted.

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

Within thirty (30) days of receipt of the Contract Form, the successful bidder shall sign and date the contract and return it to the Procuring agency.

Upon the successful Bidder's furnishing of the Performance Security pursuant to Section [2.7.5], SNDB will promptly notify each unsuccessful Bidder and will discharge his/her bid security, pursuant to ITB Section [2.4.7]

2.7.4 Signing of Contract

Within 5 Days from the date of notification of the award the successful bidder shall furnish to SNDB particulars of the person who would sign the contract on behalf of the successful bidder along with an original power of attorney executed in favour of such person.

The Contract shall be signed by the parties at Central Office SNDB, Karachi, within 10 Days of award of contract.

2.7.5 Performance Security

Within 10 DAYS of receipt of the notification of award from SNDB, the successful Bidder shall furnish to SNDB the Performance Security of 10 % of contract price which shall be valid for at least ninety (90) days beyond the date of completion of contract to cover defects liability period or maintenance period. The Performance Security shall be in the form of a pay order or demand draft or bank guarantee issued by a reputable commercial bank, acceptable to SNDB, located in Pakistan. [SPPRA Rule 39 (1)]

Failure of the successful Bidder to comply with the requirement of ITB Section [2.7.4] shall constitute sufficient grounds for the annulment of the award and forfeiture of the bid security, in which event SNDB may make the award to the next lowest evaluated Bidder or call for new bids.

The Performance Security forms at Annexure "C" shall not be completed by the bidders at the time of their bid submission. Only the successful Bidder will be required to provide Performance Security.

The Performance Security will be discharged by SNDB and returned to the Supplier not later than thirty (30) days following the date of successful completion of the Supplier's performance obligation under the Contract.

Failure of the successful Bidder to comply with requirement of ITB Clause 32 or ITB Clause 33.1 shall constitute sufficient grounds for the annulment of the award and forfeiture of the bid security, in which event the Procuring agency may make the award to the next lowest evaluated Bidder or call for new bid.

2.7.6 General Conditions of Contract

For detailed General Condition of Contract refer to Section [5.1] of this TD.

2.7.7 Special Conditions of Contract

For detailed Special Condition of Contract refer to Section [5.2] of this TD

2.7.8 Integrity Pact

The successful bidder shall upon the award of the contract execute an Integrity Pact with SNDB. *[Specimen is attached in Annexure "D"]* [SPPRA Rule 89]

2.7.9 Non-Disclosure Agreement

The successful bidder shall upon the award of the contract execute a Non-Disclosure Agreement with SNDB. *[Specimen is attached in Annexure "F"]*

3. SCOPE OF WORK / TECHNICAL SPECIFICATION

Sindh Bank requires Supply and Installation of Data Centre Web application firewall (WAF - 2). The requirement will be issued on need basis. Therefore quantity may vary depends on the requirement of the bank, accordingly bank will not be responsible if the quantity asked is not as per scope of work below and in this context no claim will be entertained. Payment will be done on supply and installation of actual numbers of items.

The prospective Supplier will provide Sindh Bank with One (01) Enterprise-Class Next Generation Web application firewall (WAF) that include the following features.

Web application firewall (WAF) REQUIREMENTS:

SPECIFICATIONS

SN#	SPECIFICATIONS	
1	Intelligent Traffic Processing:	L7 requests per second: 350K L4 connections per second: 125K L4 HTTP requests per second: 600K Maximum L4 concurrent connections: 14M Throughput: 10 Gbps L4/L7
2	Hardware Offload SSL/TLS:	ECC†: 2.1K TPS (ECDSA P-256) RSA: 2.5K TPS (2K keys) 5 Gbps bulk encryption*
3	Software Compression:	3 Gbps
4	Software Architecture:	64-bit TMOS
5	On-Demand Upgradable:	YES
6	Processor:	One 2-Core Intel Pentium processor (total 4 hyperthreaded logical processor cores)
7	Memory:	16 GB DDR4
8	Hard Drive:	1 TB Enterprise Class HDD
9	Gigabit Ethernet CU Ports:	Optional SFP
10	Gigabit Fiber Ports (SFP):	4 SX or LX (sold separately)
11	10 Gigabit Fiber Ports (SFP+):	2 SR/LR (sold separately); optional 10G copper direct attach

Policy Management

1. The WAF shall be able to automatically-built policies
2. The WAF shall be able to manually accept false positives by simple means (check box)
3. The WAF shall be able to define different policies for different applications
4. The WAF shall be able to create custom attack signatures or events
5. The WAF shall be able to customize Denial of Service policies
6. The WAF shall be able to combine detection and prevention techniques
7. The WAF shall have policy roll-back mechanism
8. The WAF shall be able to do versioning of polices
9. The WAF shall have a built-in real-time policy builder with automatic self-learning and creation of security polices
10. The WAF shall have application- ready security templates for applications - eg Microsoft Sharepoint, OWA, ActiveSync, SAP, Oracle Applications/Portal, PeopleSoft, Lotus Domino for
11. The WAF shall be capable of being restored to factory defaults
12. The WAF shall have the ability to automatically detect server technologies and suggest adding the detected server technologies to the user's security policy.
13. The WAF shall provide layered policies configuration in a hierarchical manner with a parent and child policies. This allows for quicker policy creation and learning. A security policy can be created in two ways:
    - Security Policy: This is similar to previous releases of an ASM security policy which can be applied to any relevant virtual server.
    - Parent Policy: This is a new type of policy which enables the user to create a higher level policy to act as a template for its attached child policies.
14. The WAF layered policies configuration enhancements shall have the followings:
    - Administrators can mandate that all new security policies created must be attached to a compatible

parent policy.

- All attached child policies for a parent policy are listed in the parent policy details.
- Parent policy suggestions now have a maximum score of parallel suggestions in its child policies. All locked child suggestions propagate to the parent policy. The score of the parallel suggestion in each child is shown in the parent policy pane per suggestion, with the top scoring children marked.

15. The WAF shall have an improved Policy Builder Process which has a single tabbed screen containing the configuration for a policy's General Settings, Inheritance Settings, Microservices, Attack Signatures, Threat Campaigns, and Response and Blocking Pages. The Policies List displays the name, enforcement mode, attached virtual servers and OWASP compliance.

Profile Learning Process

1. The WAF shall be able to recognize trusted hosts
2. The WAF shall be able to learn about the application without human intervention
3. The WAF shall be able to inspect policy (auditing + reporting)
4. The WAF shall be able to protect new content pages and objects without policy modifications
5. Able to provide anomaly learning of client integrity whether it is browser compared to automated web attack tool.
6. Able to configure whether the system tracks sessions based on user names, IP addresses, or session identification numbers.
7. Positive security model support - An "allow what's known" policy, blocking all unknown traffic -and data types
8. Positive security model configuration
9. Application flow
10. Dynamic Positive security model configuration maintenance
11. Built in process engine to detect evasion techniques like cross site scripting Is there an out of the box rule database available.
12. Automated regular signature updates
13. Operates in a full Proxy architecture and inline control over all traffic through the WAF
14. Ability to hide back-end application server OS fingerprinting data and application specific information
15. Ability to protect against malicious activity within and hijacking of embedded client side code (javascript, vbscript, etc...)

Dynamic Web based defenses

1. The WAF shall be able to perform cloaking e.g hiding of error pages and application error pages and even specific data
2. The WAF shall be able to perform virus checking on HTTP file uploads and SOAP attachments. Support to Anti-Virus via ICAP communication channel
3. Provide protection of AJAX-enabled applications including those that use JSON for data transfer between the client and the server. This include support in set up AJAX blocking response behavior for applications that use AJAX, so that if a violation occurs on an AJAX request, the system displays a message or redirects the application user to another location.
4. The WAF shall support protection of XML Web Services
5. The WAF shall restricts XML Web Services access to methods defined via Web Services Description Language (WSDL) or XML Schema format (XSD)
6. The WAF shall be able to perform validation for Web Services XML Documents which is WS-I compliant
7. The WAF has a XML Parser Protection, limit recursions to thwart DoS conditions, limit the numbers of elements, lengths of elements, attack signatures enforcement. In addition, it can be used to encrypt and sign documents according to the WS-Security standard.
8. The WAF shall be able to perform information display masking/scrubbing on requests and responses
9. The WAF shall support Sensitive Data Masking for personal details about users and credit cards in the following entities:
   a. HTTP Header fields, especially Authorization
   b. URL segments with personal identification using positional parameters
   c. Cookie values
   d. HTTP Request body using positional parameters
10. The WAF shall be able to monitor latency of Layer 7 (application layer) traffic to detect the spikes and anomalies in the typical traffic pattern to detect, report on, and prevent layer 7
11. The WAF shall be able to detect, report on, and prevent Layer 7 (application layer) brute force attack attempts to break in to secured areas of a web application by trying exhaustive, systematic permutations of code or username/password combinations to discover legitimate authentication credentials.
12. The WAF shall be able to detect, report on, and prevent Layer 7 (application layer) web bot doing recursive web scrapping and rapid surfing. It also has the ability to differentiate automated web attack agent from legit user. Provides the ability to customize the default list of recognized search engines, and add own site's search engine to the system's list of f. The WAF shall be able to integrate with these vulnerability testing tools - Whitehat sentinel, IBM Appscan, HP Webinspect and QualysGuard, for automated instant policy tuning. Provide unified IP address whitelists for Policy Builder trusted IP addresses, and anomaly whitelists (DoS Attack Prevention, Brute Force Attack Prevention, and Web Scraping Detection)
13. Provide GUI based control to determine the reputation of an IP address and operate (e.g. block) based on

that
reputation. The
IP reputation database is regularly updated. It detect IP reputation based on:

a. Windows Exploits: IP addresses that have exercised various exploits against Windows resources using browsers, programs, downloaded files, scripts, or operating system vulnerabilities.
b. Web Attacks: IP addresses that have launched web attacks of various forms.
c. Botnets: IP addresses representing compromised computers on the Internet that are now part of a botnet (machines that send spam messages, launch various attacks, or behave in other unpredictable ways).
d. Scanners: IP addresses that have been observed to scan ports or networks, typically to identify vulnerabilities for subsequent exploits.
e. Denial of Service: IP addresses that have launched denial of service attacks, often requests for legitimate services, but which occur at such a fast rate that targeted systems cannot respond and become overloaded or unable to service legitimate clients.
f. Reputation: IP addresses that issue HTTP requests with a low average reputation, or that request only known malware sites.
g. Phishing Proxy: IP addresses associated with phishing websites (sources that attempt to acquire information such as user names, passwords, and credit card details by masquerading as a trustworthy entity).

Detection techniques:

1. The WAF shall be able to support the following evasive detection techniques :
   a. URL-decoding
   b. Null byte string termination
   c. Self-referencing paths (i.e. use of /./ and encoded equivalents)
   d. Path back-references (i.e. use of /../ and encoded equivalents)
   e. Mixed case
   f. Excessive use of whitespace
   g. Comment removal (e.g. convert DELETE/**/FROM to DELETE FROM)
   h. Conversion of (Windows-supported) backslash characters into forward slash characters.
   i. Conversion of IIS-specific Unicode encoding (%uXXYY)
   j. Decode HTML entities (e.g. &#99;, &quot;, &#xAA;)
   k. Escaped characters (e.g. \t, \001, \xAA, \uAABB)
   l. Negative security model techniques
   m. Implemented concepts to cover vulnerabilities (OWASP based):
2. The WAF shall be able to protect against:
   a. Unvalidated input
   b. Injection flaws
   c. SQL injection
   d. OS injection
   e. Parameter tampering
   f. Cookie poisoning
   g. Hidden field manipulation
   h. Cross site scripting flaws
   i. Buffer overflows
   j. Broken access control
   k. Broken authentication and session management
   l. Improper Error Handling
   m. XML bombs/DOS
   n. Forceful Browsing
   o. Sensitive information leakage
   p. Session hijacking
   q. Denial of service
   r. Request Smuggling
   s. Cookie manipulation
3. The WAF shall be able to protect against New attack signatures
4. The WAF shall be able to protect against XML External Entities (XXE)
5. The WAF shall be able to protect against Insecure Deserialization
6. The WAF shall be able to protect against NoSQL Injection
7. The WAF shall be able to protect against Insecure File Upload
8. The WAF shall be able to protect against Server-Side Template Injection

Application Delivery and Redundancy Capabilities:

1. The WAF shall be able to support High Availability Failover via network only
2. The WAF shall be able to perform application level health check of the back end servers
3. The WAF shall be able to load balance to the back end servers (round robin, least connection, fastest response)
4. The WAF shall be able to support caching and compression in a single platform
5. The WAF shall be able to be implemented and installed on separate application delivery controller (ADC) hardware platforms
6. The WAF solution shall allow traffic pass through when the services fail. (Note that this is different from fail-open bypass)

7. The WAF shall be able to support vlan configuration through built in switch
8. The WAF shall be able to perform TCP/IP optimization
9. The WAF shall be able to perform packet filtering

SSL capabilities:

1. The WAF shall have SSL accelerators available for SSL offloading
2. The WAF shall store the certificate private key on the WAF using a secure mechanism
3. The WAF shall store the certificate private key on the WAF using a secure mechanism, and a passphrase
4. The WAF shall capable of communication to a backend application server using https
5. The WAF shall be capable of tuning the SSL parameters, such as SSL encryption method used, SSL version

Other Mandatory Features:

1. Able to support the prevention of sending or accessing cookies when unencrypted HTTP is the transport
2. Able to mitigates click-jacking attacks by instructing browsers not to load a page into a frame
3. Able to support generic scanner via a published XML schema
4. Mitigating Bots via Captcha (login wall).
5. Enable detection of anamolous traffic patterns that stem from a specific unique geo-location and allowing throttling of anomalous traffic by geo-location based on RPS counts.
6. Proactive BOT defense that provides always-on protection that prevent bot attacks driving Layer7 DOS attacks, webscrapping, and brute force attacks from ever taking place. Works with existing reactive anamoly detections. Introduces javascript challenge to slow requests down and distinguish bots before requests reach a server.
7. JS obfuscation and client side security. Adding an obfuscation mechanism to protect JS against examination or reverse engineering and tampering. The mechanism will run on the appliance as a Java background process compiling and obfuscating JS code - encrypting the code. This enhancement will ultimately hide sensitive information with JS, insert changeable data into JS files and allow a lock-free mechanism of syncing dynamically generated data including CAPTCHA and RSA key pairs.
8. The WAF shall support JSON protection.
9. The WAF shall support Single Page Application (SPA) protection by:
   - Identifying the login page based on the Action Parameter.
   - Detecting Nameless Parameters.
   - Protecting Single Page Application Form submissions.
   - Identifying the Username.
   - Recognizing the JSON Content Profile better.
10. The WAF shall provide CSRF Protection with two enforcement modes:
    - Verify CSRF Token
    - Verify Origin
11. The WAF shall support simplified custom attack signature rule writing to allow users to create rules without needing to use Snort syntax or escape common characters.
12. The WAF shall support cookie modifications for the ASM policy and Device ID cookie names.
13. The WAF shall support Wildcards in Disallowed HTTP, HTTPS and WebSocket URLs.
14. The WAF shall support monitoring of resource utilization for request queue sizes with threshold alerts triggered and sent over local log, SNMP or SMTP. In this way, users can spot
15. The WAF shall allows the addition of a list of domains allowed to send out AJAX requests with custom headers for Single Page Applications. This prevents browsers from blocking cross domain AJAX requests while still enforcing a CORS (Cross Origin Requests) policy with single page applications.
16. The WAF shall support Incidents exports in HTML format.
17. The WAF shall support Learning Suggestions exports in HTML format.
18. The WAF shall provide microservices security policy for a defined unique identifier of Hostname + URL.
19. The WAF shall provide Selective Security Live Software Updates which can receive scheduled and real time selective live updates of attack signatures, bot signatures, browser challenges,
20. The WAF shall have the OWASP Compliance Dashboard which details the coverage of each security policy for the top 10 most critical web application security risks as well as the changes
21. The WAF shall support HTTP/2 over SSL/TLS on both the client and server sides, without having to translate the client HTTP/2 traffic to HTTP/1.1 on the server-side.
22. The WAF shall log challenge failures in the event logs for Application Security and Bot Defense.
23. The WAF shall have PCI Compliance reporting which includes 2 options to automatically fix compliance issues to support PCI Compliance 3.2:
    - Encrypt transmission of cardholder data across open, public networks
    - User is forced to change password every 90 days.
24. The WAF shall have TLS fingerprints identification to distinguish between bad and good actors behind the same IP (NAT) and only block traffic from bad actors.
25. The WAF shall support Policy Change and Security Event Reporting to Continuous Integrations / Continuous Delivery (CI/CD) Servers for CI/CD Cycle Support. WAF deployment can be integrated within the user's CI/CD pipeline and user's DevOps tool chain for test and production environments. This allows the user to deploy the right WAF policy per each application

Traffic Learning & Blocking:

1. The WAF must able to configure a list of Allowed File Types for your web application
2. The WAF must be able to allow or disallow specific file type
3. The WAF must able to configure a list of Allowed URLs for your web application

4. The WAF must able to configure a list of Allowed Parameters for your web application
5. The WAF must able to configure a list of Allowed Cookies for your web application
6. The WAF must able to configure a list of Allowed HTTP Methods for your web application
7. The WAF must capable of blocking specific list of HTTP methods
8. The WAF must able to configure a list of Allowed Redirection Domains for your web application
9. The WAF must be able to enforce maximum length of following HTTP request parameters
   - URL Length
   - Query String (URL parameters) Length
   - Request Length
   - POST data size
10. The WAF must be able to enforce specific HTTP headers and values to be present in client requests
11. The WAF must support HTML5 Cross-Domain Request Enforcement to enable one website to access the resources of another website using JavaScript.
12. The WAF must be able to enforce specific HTTP headers and values to be present in client requests
13. The WAF must capable of defining parameters of own attack detection signatures and be alerted when thresholds for these are passed
14. The WAF must automatically download and apply new signatures to ensure up-to-date protection
15. The WAF must operate in a full Proxy architecture and inline control over all traffic
16. The WAF must be able to to hide back-end application server OS fingerprinting data and application specific information
17. The WAF must be able to protect against malicious activity within and hijacking of embedded client side code (javascript, vbscript, ect...)
18. The WAF must be able to mitigate DoS vectors focusing on protocol weaknesses of HTTP such as:
    - Slowloris
    - Slow Post
    - Hash DoS
    - HTTP Get Flood
19. The WAF must be able to detect DoS attacks by monitoring the average number of transactions per client IP addresses or individual requested URLs per second
20. The WAF must be able to detect DoS attacks by monitoring the average time it takes for the backend server to repspond to a specific URL. The WAF evaluates the response traffic from
21. the server to understand the Server Stress level to determine a DoS attack
22. The WAF must be able to detect, report on, and prevent Layer 7 (application layer) brute force attack attempts to break in to secured areas of a web application by trying exhaustive, systematic permutations of code or username/password combinations to discover legitimate authentication credentials.
23. The WAF must be able to stop non-human attackers by presenting a character recognition challenge to suspicious users. This CAPTCHA challenge will be presented after the system detects one or more of the following issues:
    - A suspicious IP address
    - Requests from a suspicious country
24. The WAF must be able to mitigate traffic from countries that send suspicious traffic.
25. The WAF must be able to inject a JavaScript challenge instead of the original response in order to test whether the client is a legitimate browser or a bot.
26. The WAF must be able to protect Web Scraping from following criteria: Bot detection (Mouse and Keyboard activity, and Rapid Surfing detection), Fingerprinting, Suspicious clients and
27. The WAF must support IP address whitelist and blacklist
28. The WAF must have capability of detecting non-browser based BOTs as part of the WAF advance BOTs detection capabilities
29. The WAF shall support the ability to disable individual attack signatures on HTTP headers, wildcard URLs and wildcard headers (*).
30. The WAF shall use proprietary correlation algorithms to aggregate reported events from non-staged traffic into user-understandable security issue incidents for quicker review and user
31. The WAF shall support "Potential Disallowed Files Type" List which may be seen in malicious requests, such as information leakage and remote code execution.
32. The WAF shall come with a preconfigured list which users can add to. T
33. he WAF shall automatically check all traffic for all policies against this list and can generate suggestions to amend a policy to add or remove
34. The WAF shall monitor and make suggestions for deletion on unobserved (inactive) entities similar to its suggestions for addition on observed entities in the Policy Building Process.
35. The WAF shall support client reputation mechanism which identifies bad sources, e.g. source IPs or device IDs, and contributes to an enhanced security policy enforcement and the prevention of false positive alerts. The Client Reputation score is used to prevent learning from malicious sources, e.g. vulnerability scanners, and improve the learning speed from The WAF shall support URL Positional Parameters as part of global parameters. The URL with positional parameters is a non-pure wildcard, e.g. /p/* or */cart/*/item/php.

<u>Behavioral DoS:</u>

1. The WAF shall support BADoS Unified Server Health Check Mechanism Based on L7 Analysis. The same virtual server predictive latency is now used for BADoS and Layer 7 DoS. This allows them to have the same trigger for stress and attack detection.
2. The WAF shall support BADoS DDoS Mitigation Based on Behavior Analysis and Integration with Whitelist. This provides administrators with the ability to exclude whitelist members from statistics

collection,
anomaly
detection and mitigation. This feature also supports anomaly detection of X-Forwarded-For (XFF) HTTP headers.

3. The WAF shall provide BADoS automatic generation of Attack Request Signatures. Attackers are identified and marked as bad actors after their first appearance. This allows better policy enforcement when an attacker reappears thus sparing the remitigation process from BADoS.
4. The WAF shall support automatic threshold tuning in Layer 7 DoS TPS-based Detection and Stress-based Detection.
5. In TPS-based Detection, a single global threshold is calculated for each of the following entity types:
   - Device ID
   - Source IP
   - URL
   - Site Wide
6. In Stress-based Detection, the following thresholds are calculated:
   - Device ID: Thresholds for up to the top 50 Device IDs are calculated and an additional threshold for all other Device IDs.
   - Source IP: Thresholds for up to the top 100 source IPs are calculated and an additional threshold for all other source IPs. - URLs: Thresholds for up to the top 500 source URLs are calculated and an additional threshold for all other URLs.
   - Site Wide: Single threshold
7. The WAF shall provide accelerated attack signature detection and mitigation for L4 DoS to handle very strong high rate DoS attacks.
8. The WAF shall be able to provide DoS-L7 Traffic Passive Monitoring via Switched Port Analyzer.

Unified Bot Defense (Proactive Bot Defense & Anti-Bot Mobile SDK):

1. The WAF shall support logging and reporting for Proactive Bot Defense which includes:
   - A dedicated Bot Defense Request Log that displays each HTTP request along with its attributes.
   - A Bot Defense Logging Profile to provide basic filtering capabilities in the Request Log and Remote Log. - Additional info and Blocking Page configuration in iRule.
   - Transaction Outcome charts with filtering and drill-down capabilities.
2. The WAF shall detect brute force attacks from sources identified by Username, Device ID or Source IP. The brute force functionality shall include:
   - Enforcement actions: CAPTCHA, Client Side Integrity, Honeypot and Drop.

   - Prevention for CAPTCHA bypass and Client Side Integrity bypass. - Distributed brute force attack protection.
   - Detection of Credentials Stuffing attacks using a dictionary of leaked or stolen credentials.
   - Prevention and Mitigation Duration are in minutes.
3. The WAF shall detect mobile application bots by identifying that the access is indeed a mobile app access and that the application is indeed untampered with. The WAF shall be able to extract a unique, non-Java Script, fingerprint for each mobile application instance and report client traffic composition per application for any given time period and what applications are used and the top URLs accessed. Mobile application detection is supported via a Software Development Kit (which requires minimal development and integration) and is supported
4. The WAF shall provide an Unified Anti-Bot Detection and Protection which covers bot signatures and proactive bot defense, and web scraping within a single Bot Defense profile.
5. The WAF shall have HTTP Header Sequence Behavioral Metric which can be used as a signature metric in distinguishing between real browsers and Bad Actor bots that have inaccurately
6. The WAF shall support CAPTCHA Sound to provide accessibility to the visually impaired. This default CAPTCHA response sound file can be replaced with a custom sound file.

DataSafe (Application Level Encryption):

1. The WAF shall support Single Page Applications (SPA) view for Application Level Encryption configuration on a login page.
2. The WAF shall allow parameter configuration in Application Level Encryption (DataSafe) based on all types of HTTP methods.
3. The WAF shall be able to create logging profiles to log information on client attempts to login to your protected website, and to log information on alerts sent by the BIG-IP system.
4. The WAF shall detect attempts to steal a user’s password in the web browser when Password Exfiltration Detection is enabled on a protected URL. For this detection to be active, your URL must have a parameter set as Identify as Username and at least one parameter set as Substitute Value.

API Security:

1. The WAF shall provide Public APIs Protection by loading the Customer-specific OpenAPI files, which are in Swagger format, to the platform to automatically create a security policy
2. The WAF shall support JSON schema for user REST endpoints which can be uploaded to a JSON profile.
3. The WAF shall allow users to use Guided Configuration in ASM to configure API Security to protect API calls.
4. The WAF shall provide a API Protection Dashboard which displays API server health including security events that were flagged, such as web application attacks, bad source IP addresses, and malicious transactions. Users can use the dashboard for troubleshooting API Security.
5. The WAF shall support OpenAPI 3.0 Protection.

Delivery Time

Within 8 weeks

3 FINANCIAL PROPOSAL

PRICE SCHEDULE

(Applicable for the year 2021-2022)

Name of Bidder ____

S.NO	Item	Unit Price	Quantity	Amount (PKR)
1	Web application firewall (WAF-2)		1	
	***Total Amount (In PKR)**			

*** This amount will be considered as only the "Bid Offered". Whereas be apprised that the successful bidder will be the one whose "Evaluated Bid" is the lowest. (For further clarification refer Note. 6 below).**

Note

1. The total cost must include all applicable taxes, duties and other charges as mentioned in the description column, Stamp duty (as applicable under Stamp Act 1989), delivery charges upto Sindh Bank Limited branches on Countrywide basis
2. No advance payment for supply of goods will be made, bills are only be processed for necessary payment on receipt of certificate of delivery/satisfaction from the branch manager.
3. **Calculation of Bid Security**.5% of the Grand Total Amount of the Financial Proposal will be submitted along with tender as Bid Security
4. In case it is reviled at any stage after supply of the goods/items that the asked specification of the tender have not been met, the amount of the supply of that specific goods will be fined to the vendor with appropriate action as deem necessary by the procurement committee.
5. Qualified company will also be bound to sign a bond/undertaking that in case of any observation arising in respect of quality of the goods within the warranty period, the company will be liable to address it at his own cost, non-compliance of the same will result into initiation of a case against the company for non-commitment or cancellation of tender as will be decided by the Procurement Committee.
6. Lowest evaluated bid is going to be the criteria for award of contract rather than considering the lowest offered bid, encompassing the lowest whole sum cost which the procuring agency has to pay for the duration of the contract. SPPRA Rule 49 may please be referred.
7. All conditions in the contract agreement attached as Annexure G are part of this tender document.
8. The tender will be considered cancelled if the contract agreement after due signature is not submitted with Admin Office after 5 days of completion of bid evaluation report hoisting period 3 days) on SPPRA website.
9. In case financial bids are the same, the successful bidder will be the one who has acquired more marks in the technical evaluation.
10. In case of over writing/cutting/use of Blanco is found in the Financial Bid document, the bid will be taken as null & void however if the figures are readable and are also duly signed only then, bid will be accepted.
11. Contract agreement will be executed after deposit of 5% performance security of the total tender amount in shape of Pay Order/Bank Guarantee in favor of Sindh Bank Limited.
12. Quality is ensured. In case it is revealed at any stage after supply of the items that the asked specifications of the tender have not been met, the performance security will be forfeited.
13. Free backup facility in case the item is reported defective.
14. Goods to be delivered have to be packed in such a way that no damage is reported by the branch on delivery. In case of any such complaint is received the bidder will replace that item at his own cost.
15. If the obligation of warranty period are not met or delayed, the repair etc. requirement on this account will be deducted from the performance security / upcoming payment due to supplier
16. *Payment will be made in Pak Rupee.*

Note. There can be subsequent modification or amendment to this specific tender for which it is advised to keep yourself abreast with the notification being hoisted on Sindh Bank Ltd. & SPPRA website regularly.

Signature & Stamp of Bidder ____

5 Contract

5.1 Conditions of Contract

5.1.1 Definitions

In this contract, the following terms shall be interpreted as indicated:

Applicable Law" means the Sindh Public Procurement Act 2009 and the Sindh Public Procurement Rules 2010.(Amended 2019)

"Procuring Agency" or "PA" means SNDB Contractor.

"Contract" means the Contract signed by the Parties and all the attached documents listed in its Clause 1 that is General Conditions (GC), and the Special Conditions (SC).

"Contract Price" means the price to be paid for the performance of the Services. "Effective Date" means the date on which this Contract comes into force.

"GC" mean these General Conditions of Contract.

"Government" means the Government of Sindh.

"Currency" means Pak Rupees.

"Member" means any of the entities that make up the joint venture/consortium/association, and "Members" means all these entities.

"Party" means the PA or the Contractor, as the case may be, and "Parties" means both of them.

"Personnel" means persons hired by the Contractor or by any Sub- Contractors and assigned to the performance of the Services or any part thereof.

"SC" means the Special Conditions of Contract by which the GC may be amended or supplemented.

"Services" means the services to be performed by the Contractor pursuant to this Contract, as described in the scope of services.

"In writing" means communicated in written form with proof of receipt.

5.1.2 Law Governing Contract

This Contract, its meaning and interpretation, and the relation between the Parties shall be governed by the laws of the Islamic Republic of Pakistan.

5.1.3 Notice

- Any notice, request or consent required or permitted to be given or made pursuant to this Contract shall be in writing. Any such notice, request or consent shall be deemed to have been given or made when delivered in person to an authorized representative of the

- Party to whom the communication is addressed, or when sent to such Party at the address specified in the SC.

- A Party may change its address for notice hereunder by giving the other Party notice in writing of such change to the address specified in the SC.

5.1.4 Authorized Representative

Any action required or permitted to be taken, and any document required or permitted to be executed under this Contract by the SNDB or the Supplier may be taken or executed by the officials.

5.1.5 Taxes and Duties

The Supplier, Sub-Suppliers, and their Personnel shall pay such direct or indirect taxes, duties, fees, and other impositions levied under the Applicable Law as specified in the SC, the amount of which is deemed to have been included in the Contract Price.

5.1.6 Effectiveness of Contract

This Contract shall come into effect on the date the Contract is signed by both Parties. The date the Contract comes into effect is defined as the Effective Date.

5.1.7 Expiration of Contract

Unless terminated earlier pursuant to Clause GC 5.1.7 hereof, this Contract shall expire at the end of such time period after the Effective Date as specified in the SC.

5.1.8 Modifications or Variations

Any modification or variation of the terms and conditions of this Contract, including any modification or variation of the scope of the Services, may only be made by written agreement between the Parties. However, each Party shall give due consideration to any proposals for modification or variation made by the other Party.

5.1.9 Force Majeure

The failure on the part of the parties to perform their obligation under the contract will not be considered a default if such failure is the result of natural calamities, disasters and circumstances beyond the control of the parties.

No Breach of Contract

The failure of a Party to fulfil any of its obligations under the contract shall not be considered to be a breach of, or default under, this Contract insofar as such inability arises from an event of

Force Majeure, provided that the Party affected by such an event (a) has taken all reasonable precautions, due care and reasonable alternative measures in order to carry out the terms and conditions of this Contract, and (b) has informed the other Party as soon as possible about the occurrence of such an event.

Extension of Time

Any period within which a Party shall, pursuant to this Contract, complete any action or task, shall be extended for a period equal to the time during which such Party was unable to perform such action as a result of Force Majeure.

Termination

Termination by SNDB

The SNDB may terminate this Contract in case of the occurrence of any of the events specified in paragraphs (a) through (f) of this Clause GC 5.1.10.1. In such an occurrence the SNDB shall give a not less than thirty (30) days' written notice of termination to the Supplier, and sixty (60) days' in the case of the event referred to in (e).

a. If the Supplier does not remedy the failure in the performance of their obligations under the Contract, within thirty (30) days after being notified or within any further period as the SNDB may have subsequently approved in writing;

b. If the Supplier becomes insolvent or bankrupt;

c. If the Supplier, in the judgment of the SNDB has engaged incorrupt or fraudulent practices in competing for or in executing the Contract;

d. If, as the result of Force Majeure, the Supplier(s) are unable toper form a material portion of the Services for a period of not less than sixty (60) days; and

e. If the SNDB, in its sole discretion and for any reason whatsoever, decides to terminate this Contract.

Termination by the Supplier

The Suppliers may terminate this Contract, by not less than thirty (30) days' written notice to the SNDB, such notice to be given after the occurrence of any of the events specified in paragraphs (a) through (c) of this Clause GC 5.1.10.2

a. If the SNDB fails to pay any money due to the Supplier pursuant to this Contract without Suppliers fault.

b. If, as the result of Force Majeure, the Supplier is unable to perform a material portion of the Services for a period of not less than sixty (60) days

Payment upon Termination

Upon termination of this Contract pursuant to Clauses GC 5.1.10.1 or GC 5.1.10.2, the SNDB shall make the following payments to the Supplier:

a. Payment for Services satisfactorily performed prior to the effective date of termination;

b. except in the case of termination pursuant to paragraphs (a) through (c) of Clause GC 5.1.10.1, reimbursement of any reasonable cost incident to the prompt and orderly termination of the Contract, including the cost of the return travel of the Personnel and their eligible dependents.

Good Faith

The Parties undertake to act in good faith with respect to each other's rights under this Contract and to adopt all reasonable measures to ensure the realization of the objectives of this Contract.

Settlement of Disputes

Amicable Settlement

The Parties agree that the avoidance or early resolution of disputes is crucial for a smooth execution of the Contract and the success of the assignment. The Parties shall use their best efforts to settle amicably all disputes arising out of or in connection with this Contract or its interpretation.

Arbitration

If the SNDB and the Supplier fail to amicably settle any dispute arising out of or in connection with the Contract within ten (10) days of commencement of such informal negotiations, the dispute shall be referred to arbitration of two arbitrators, one to be appointed by each party, in accordance with the Arbitration Act, 1940. Venue of arbitration shall be Karachi, Pakistan and proceedings of arbitration shall be conducted in English.

Data Ownership

The data in the implemented Computer System shall at all times remain the exclusive property of SNDB. The Supplier is hereby required to transfer all necessary passwords, access codes or other information required for full access to the data to SNDB upon successful commissioning of the Computer System and should not be available to any other party including the employees of the supplier.

Obligations of the Supplier

The Supplier shall perform the Services and carry out their obligations hereunder with all due diligence, efficiency and economy, in accordance with generally accepted professional standards and practices, and shall observe sound management practices, and employ appropriate technology and safe and effective equipment, machinery, materials and methods. The Supplier shall always act, in respect of any matter relating to this Contract or to the Services, as faithful advisers to the SNDB, and shall at all times support and safeguard the SNDB legitimate interests in any dealings with Sub-Suppliers or third Parties.

Conflict of Interest

The Supplier shall hold the SNDB’s interests paramount, without any consideration for future work, and strictly avoid conflict with other assignments or their own corporate interests.

Confidentiality

Except with the prior written consent of the SNDB, the Supplier and the Personnel shall not at any time communicate to any person or entity any confidential information acquired in the course of the Services, nor shall the Supplier and the Personnel make public the recommendations formulated in the course of, or as a result of, the Services.

5.2 Special Conditions of Contract

The following Special Conditions of Contract shall supplement the General Conditions of Contract. Whenever there is a conflict, the provisions herein shall prevail over those in the General Conditions of Contract.

5.2.1 Performance Security

The amount of performance security shall be ten (10 %) percent of the Contract Price

5.2.2 Payment

The payment to be made to the Supplier under this Contract shall be made in accordance with the payment schedule as shall be agreed between SNDB and the Supplier.

a. All advance payment (if any) will be made against valid bank guarantee(s).

b. SNDB will effect payment within 30 days on satisfactory delivery of services, upon submitting the invoice under above conditions.

5.2.3 Price

Schedule of prices shall be as fixed in the Contract.

Annexure "A"

6. BID FORM

FORM OF BID

Tender Reference No……………………………. Dated: __________, 2020

To,

Head of Information Technology
SINDH BANK LIMITED
HEAD OFFICE
Basement-2 Floor, Federation House,
Abdullah Shah Ghazi Road,
Clifton,
Karachi 75600

Gentleman,

Having examined the bidding documents, the receipt of which is hereby duly acknowledged, we, the undersigned, offer, in conformity with the said bidding documents for the sum of currency_____________________ [total bid amount in words and figures].

We understand that all the Annexures attached hereto form part of this Bid.

We undertake, if our Bid is accepted, [to provide goods/work/related service], that will be in accordance with the terms defined in the proposal and /or contract.

Our firm, including any subcontractors or suppliers for any part of the Contract, have nationalities from the following eligible countries
____.

If our Bid is accepted, we will obtain the Bank Guarantee/Pay order in a sum equivalent to ten percent (10%) of the Contract Price for the due performance of the Contract, in the form prescribed by SNDB.

We agree to abide by this Bid for a period of ninety (90) days from the date fixed for Bid Opening and it shall remain binding upon us and may be accepted at any time before the expiration of that period.

Until a formal Contract is prepared and executed, this Bid, together with your written acceptance thereof and your notification of award, shall constitute a binding Contract between us.

Commissions or gratuities, if any, paid or to be paid by us to agents relating to this Bid and to contract execution if we are awarded the contract, are listed below:

We understand that you are not bound to accept the lowest or any Bid you may receive.

Name & Address of Bidder in Block Capital

____

____

Dated this ___________ day of ________ 2020

___________________   _____________________

[Signature]   ***[In the Capacity of]***

Duly authorized to sign Bid for and on behalf of ___________________________

Witness;

Signature;_______________________

Name: _______________________

Address:---

Occupation: --

Annexure "B"

7. BID SECURITY FORM

Whereas [name of the Bidder] has submitted its bid dated [date of submission of bid] for the supply of Disinfectant Sanitizer Foam & Surgical Face Mask and Surgical Gloves.

KNOW ALL PEOPLE by these presents that WE [name of bank] of [name of country], having our registered office at [address of bank] (hereinafter called "the Bank"), are bound unto Sindh Bank (hereinafter called "the Purchaser") in the sum of Rupees________________ for which payment well and truly to be made to the said Purchaser, the Bank binds itself, its successors, and assigns by these presents. Sealed with the Common Seal of the said Bank this ____ day of ___ 2020.

THE CONDITIONS of this obligation are:

1. If the Bidder withdraw its Bid during the period of bid validity specified by the Bidder on the Bid Form; or

2. If the Bidder, having been notified of the acceptance of its Bid by the Sindh Bank during the period of bid validity:

    a. fails or refuses to execute the Contract, if required; or

    b. fails or refuses to furnish the performance security, in accordance with the Instructions to Bidders;

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

This guarantee will remain in force up to and including twenty eight (28) days after the period of bid validity and any demand in respect thereof shall reach the Bank not later than the above date.

[Signature and Seal of the Bank]

Annexure "C"

8. PERFORMANCE SECURITY FORM

To,

Head of Information Technology
SINDH BANK LIMITED
HEAD OFFICE
Basement-2 Floor, Federation House,
Abdullah Shah Ghazi Road,
Clifton,
Karachi 75600

WHEREAS [name of Supplier] (hereinafter called "Supplier" or "Contractor") has undertaken, in pursuance of Contract No. _____ [reference number of the contract] dated ____ 2020 to __________ [details of task to be inserted here] (hereinafter called "the Contract").

AND WHEREAS we have agreed to give the Supplier / Contractor guarantee as required pursuant to the budding document and the contract:

THEREFORE WE hereby affirm that we are Guarantors and responsible to you, on behalf of the Supplier / Contractor, up to a total of [amount of the guarantee in words and figures], and we undertake to pay you, upon your first written demand declaring the Supplier / Contractor to be in default under the Contract and without cavil or argument, any sum or sums within the limits of [amount of guarantee] as aforesaid, without your needing to prove or to show grounds or reasons for your demand or the sum specified therein.

This guarantee is valid until the _____ day of _______2020.

<u>Signature and Seal of the Guarantors</u>

Name of Bank

Address

Date

Annexure "D"

9. INTEGRITY PACT

Declaration of Fees, Commissions and Brokerage etc. Payable by the Suppliers of Services Pursuant To Rule 89 Sindh Public Procurement Rules Act, 2010

________________________ [the Supplier] hereby declares that it has not obtained or induced the procurement of any contract, right, interest, privilege or other obligation or benefit from Government of Pakistan (GoP) or any administrative subdivision or agency thereof or any other entity owned or controlled by it (GoP) through any corrupt business practice.

Without limiting the generality of the foregoing, [the Supplier] represents and warrants that it has fully declared the brokerage, commission, fees etc. paid or payable to anyone and not given or agreed to give and shall not give or agree to give to anyone within or outside Pakistan either directly or indirectly through any natural or juridical person, including its affiliate, agent, associate, broker, consultant, director, promoter, shareholder, sponsor or subsidiary, any commission, gratification, bribe, finder's fee or kickback, whether described as consultation fee or otherwise, with the object of obtaining or inducing the procurement of a contract, right, interest, privilege or other obligation or benefit in whatsoever form from GoP, except that which has been expressly declared pursuant hereto.

[The Supplier] certifies that it has made and will make full disclosure of all agreements and arrangements with all persons in respect of or related to the transaction with GoP and has not taken any action or will not take any action to circumvent the above declaration, representation or warranty. [The Supplier] accepts full responsibility and strict liability for making any false declaration, not making full disclosure, misrepresenting facts or taking any action likely to defeat the purpose of this declaration, representation and warranty. It agrees that any contract, right, interest, privilege or other obligation or benefit obtained or procured as aforesaid shall, without prejudice to any other right and remedies available to GoP under any law, contract or other instrument, be voidable at the option of GoP.

Notwithstanding any rights and remedies exercised by GoP in this regard, [the Supplier] agrees to indemnify GoP for any loss or damage incurred by it on account of its corrupt business practices and further pay compensation to GoP in an amount equivalent to ten times the sum of any commission, gratification, bribe, finder's fee or kickback given by [the Supplier] as aforesaid for the purpose of obtaining or inducing the procurement of any contract, right, interest, privilege or other obligation or benefit in whatsoever form from GoP.

For and On Behalf Of

____

Signature: _______________________

Name: _______________________

NIC No: _______________________

Annexure "E"

10. SCHEDULE OF OPENING AND SUBMISSION OF BID

For details refer to Newspaper Advertisement published on the subject matter.

Annexure "F"

11. FORM OF CONTRACT (Non-Disclosure Agreement)

This Mutual Non-Disclosure Agreement ("Agreement") is made and entered into between Sindh Bank Limited, and [Supplier Name], individually referred to as a 'Party' and collectively referred to as the 'Parties'. The Parties wish to exchange Confidential Information (as defined below in Section 2) for the following purpose(s): a) to evaluate whether to enter into a contemplated business transaction; and b) if the Parties enter into an agreement related to such business transaction, to fulfil each Party's confidentiality obligations to the extent the terms set forth below are incorporated therein (the "Purpose").

The Parties have entered into this Agreement to protect the confidentiality of information in accordance with the following terms:

1. The Effective Date of this Agreement is________________________ 2020.

2. In connection with the Purpose, a Party may disclose certain information it considers confidential and/or proprietary ("Confidential Information") to the other Party including, but not limited to, tangible, intangible, visual, electronic, present, or future information such as:

   - Trade secrets;

   - Financial information, including pricing;

   - Technical information, including research, development, procedures, algorithms, data, designs, and know-how;

   - Business information, including operations, planning, marketing interests, and products;

   - The terms of any agreement entered into between the Parties and the discussions, negotiations and proposals related thereto; and

   - Information acquired during any facilities tours.

3. The Party receiving Confidential Information (a "Recipient") will only have a duty to protect Confidential Information disclosed to it by the other Party ("Discloser"):

   - If it is clearly and conspicuously marked as "confidential" or with a similar designation;

   - If it is identified by the Discloser as confidential and/or proprietary before, during, or promptly after presentation or communication; or

   - If it is disclosed in a manner in which the Discloser reasonably communicated, or the Recipient should reasonably have understood under the circumstances, including without limitation those described in Section 2 above, that the disclosure should be treated as confidential, whether or not the specific designation "confidential" or any similar designation is used.

4. A Recipient will
   use the Confidential Information only for the Purpose described above. A Recipient will use the same degree of care, but no less than a reasonable degree of care, as the Recipient uses with respect to its own information of a similar nature to protect the Confidential Information and to prevent:

   - Any use of Confidential Information in violation of this agreement; and/or

   - Communication of Confidential Information to any unauthorized third parties. Confidential Information may only be disseminated to employees, directors, agents or third party contractors of Recipient with a need to know and who have first signed an agreement with either of the Parties containing confidentiality provisions substantially similar to those set forth herein.

5. Each Party agrees that it shall not do the following, except with the advanced review and written approval of the other Party:

   - Issue or release any articles, advertising, publicity or other matter relating to this Agreement (including the fact that a meeting or discussion has taken place between the Parties) or mentioning or implying the name of the other Party; or

   - Make copies of documents containing Confidential Information.

6. This Agreement imposes no obligation upon a Recipient with respect to Confidential Information that:

   - Was known to the Recipient before receipt from the Discloser;

   - Is or becomes publicly available through no fault of the Recipient;

   - Is independently developed by the Recipient without a breach of this Agreement;

   - Is disclosed by the Recipient with the Discloser's prior written approval; or

   - Is required to be disclosed by operation of law, court order or other governmental demand ("Process"); provided that (i) the Recipient shall immediately notify the Discloser of such Process; and (ii) the Recipient shall not produce or disclose Confidential Information in response to the Process unless the Discloser has: (a) requested protection from the legal or governmental authority requiring the Process and such request has been denied, (b) consented in writing to the production or disclosure of the Confidential Information in response to the Process, or (c) taken no action to protect its interest in the Confidential Information within 14 business days after receipt of notice from the Recipient of its obligation to produce or disclose Confidential Information in response to the Process.

7. EACH DISCLOSER WARRANTS THAT IT HAS THE RIGHT TO DISCLOSE ITS CONFIDENTIAL INFORMATION. NO OTHER WARRANTIES ARE MADE. ALL CONFIDENTIAL INFORMATION DISCLOSED HEREUNDER IS PROVIDED "AS IS".

8. Unless the Parties otherwise agree in writing, a Recipient’s duty to protect Confidential Information expires [YEARS] from the date of disclosure. A Recipient, upon Discloser’s written request, will promptly return all Confidential Information received from the Discloser, together with all copies, or certify in writing that all such Confidential Information and copies thereof have been destroyed. Regardless of whether the Confidential Information is returned or destroyed, the Recipient may retain an archival copy of the Discloser’s Confidential Information in the possession of outside counsel of its own choosing for use solely in the event a dispute arises hereunder and only in connection with such dispute.

9. This Agreement imposes no obligation on a Party to exchange Confidential Information, proceed with any business opportunity, or purchase, sell, license and transfer or otherwise make use of any technology, services or products.

10. Each Party acknowledges that damages for improper disclosure of Confidential Information may be irreparable; therefore, the injured Party is entitled to seek equitable relief, including injunction and preliminary injunction, in addition to all other remedies available to it.

11. This Agreement does not create any agency or partnership relationship. This Agreement will not be assignable or transferable by Participant without the prior written consent of the other party.

12. This Agreement may be executed in two or more identical counterparts, each of which shall be deemed to be an original including original signature versions and any version transmitted via facsimile and all of which taken together shall be deemed to constitute the agreement when a duly authorized representative of each party has signed the counterpart.

13. This Agreement constitutes the entire agreement between the parties with respect to the subject matter hereof, and supersedes any prior oral or written agreements, and all contemporaneous oral communications. All additions or modifications to this Agreement must be made in writing and must be signed by the Parties. Any failure to enforce a provision of this Agreement shall not constitute a waiver thereof or of any other provision.

Sindh Bank Limited

Registered Address:

Name: ___________________________________

Signature: _______________________________

Title: ____________________________________

Date: ____________________________________

Company Name:

Registered Address:

Name: ___________________________________

Signature: _______________________________

Title: ____________________________________

Date: ____________________________________

Annexure "G"

12. AGREEMENT

This Agreement is made on this_________________ day of________________________ ,
Between Sindh Bank Limited having its head office at 3rd Floor, Federation House, Clifton, Karachi (hereinafter called the Purchaser)

And

M/S.__________________________ having its registered office at ____________________________ (Here in after called the Vendor).

WHEREAS the Vendor is the dealer/supplier/manufacturer of ______________________ (Goods).

AND WHEREAS the Bank is inclined to purchase the Goods as detailed below on the terms and conditions laid down hereinafter for the supply of of Disinfectant Sanitizer Foam & Surgical Face Mask and Surgical Gloves for the BANK of total sum Amounting Rs. ____________ .

Detail of items are as follows.

S.No	Product	Quantity	Unit Price PKR	Total Price (PKR)

Terms & Conditions:

1. The vendor will provide the performance security in the form acceptable to the Bank. for the 10% of the order value for the period of 90 days from the date of Submission of performance security . In case Vendor does not fulfil its commitments the bank reserves the right to enforce the performance security. All terms & condition of the tender documents are part of this agreement

2. The vendor shall supply Goods as per specifications and upon the recommendations of the Technical / Standardized Committee appointed by the Bank within __________ weeks from the date of receipt of Purchase Order.

3. The bank will have the option to enforce the performance bond on happening of any one or all the following events.

a. If the vendor fails to deliver the Goods as per agreed Schedule.
b. If the vendor fails to get the Goods inspected by the Technical Committee.
c. If the Goods supplied by the vendor fails to perform as per Banks requirement.

4. The Vendor is obliged and bound to replace any or all parts broken or damaged in transit at his own cost and risk and shall deliver all the goods in good and sound condition.

5. The warranty of the goods is One year comprehensive onsite from the date of delivery.

6. The warranty will be effective while the Goods remain in the premises of the Bank and the Bank will not be responsible to send the goods to the vendor site. In case however if any portion of goods required to be shifted to vendor's site, vendor will provide equivalent backup during the warranty period.

7. Vendor agrees to maintain adequate inventory of the goods so that the replacement is available within 24 hours, if any fault arises in the goods during the warranty period. In case the effected part is not available, then the vendor will provide backup goods of the same product or better till the resolution of the fault, without any extra cost to the bank. The vendor will provide 12 Month Principal Back Warranty to cover Advance Goods Replacement, 24x7 Technical Assistance, Software Updates & Patches & Support.

8. The vendor also undertakes to bear all kind of taxes i.e. Stamp duty/ Services Charges/Professional Tax / Sales Tax Invoice, Income Tax, Zila / Octroi Tax (if any) and all other incidental charges etc, up to the place of destination.

9. The Bank reserves the right to Test/Check the goods to ensure that it is provided as per specification in the tender document. For any discrepancies, the Bank reserve the right to forfeit full security deposit/ cancel the order for the supply and bring the vendor on black list of the Bank forever. The decision of the Bank shall be final and binding upon the vendor.

10. In the event of the default on the part of the vendor, in the performance of any condition of the contract and if such default is not remedied within 3 days it shall be lawful for the Bank to enforces full or part of the Earnest money / Performance Security and or cancel the whole part of the supply order with vendor and the decision of the Bank will be the final and legally binding on the vendor.

11. Proportionate payments against supply of goods will be made within Thirty days from the goods delivery date.

12. In case of any dispute at any point the matter will be settled amicably. If the parties do not reach a settlement the dispute will be referred to the Complaint Redressal Committee for Dispute Resolution.

13. Delivery will be made by the vendor at different locations prescribed by the Bank.

14. In case of failure to supply the requisite within 7 working days after the delivery time, as described under clause no 2 of this agreement, Rs.1,000/- per day may be charged.

14. The term of this agreement shall be for the period of _______ year, commencing from the date of signing of this agreement. Extendable up to three years.

15. CONFIDENTIALITY

i. **Confidential Information.** For the purposes of this Agreement, the term “Confidential Information” shall mean any information comes in possession of M/S ___________on and its personnel during normal course of business / Services shall be the property of the SNDB at all times and / or any of the SNDB’s communications, whether in oral, written, graphic, magnetic, electronic, or other form, that is either conspicuously marked “confidential” or “proprietary,” or is known to be confidential or proprietary, or is of a confidential or proprietary nature, and that is made in the course of discussions, studies, or other work undertaken shall be kept confidential by M/S ____________________.

ii. M/S _______________. Acknowledges that the SNDB is under strict confidentiality obligations with regard to all the information and affairs of its Customers. Therefore, Nedo Corporation COMPANY shall not disclose any data, information or other affairs of SNDB’s customers which may come to the knowledge of M/s_______________ in providing the above services. _________________undertakes to obtain from its employees involved in the Services to provide written undertakings to maintain the confidentiality obligations of M/S ________________________under this Agreement.

iii. In the event of breach of this clause, M/S__________________. shall be liable to pay damages to the SNDB and indemnifies the SNDB against any injury arising out of any breach of this clause by the SNDB.

iv. This clause shall survive termination of the Agreement.

16. INDEMNIFICATION.

v. M/S__________________________. (the “Indemnifier”) agrees that it shall indemnify, defend, and hold harmless the SNDB and its parent, subsidiaries, affiliates, successors, and assigns and their respective directors, officers, employees and agents (collectively, the "Indemnities") from and against any and all liabilities, claims, suits, actions, demands, settlements, losses, judgments, costs, damages and expenses (including, without limitation, reasonable attorneys', accountants' and experts' fees) arising out of or resulting from, in whole or in part: (i) any act, error or omission, whether intentional or unintentional, by the Indemnifier or its officers, directors, employees, or sub-administrators, related to or arising out of the business covered by this Agreement, or (ii) an actual or alleged breach by the Indemnifier of any of its representations, warranties or covenants contained in this Agreement (including, without limitation, any failure of Indemnifier to comply with applicable local, state, provincial or federal regulations concerning Indemnifier’s performance under this Agreement).

i. This Article shall survive termination of this Agreement.

17. Ensuring Access to SBP

M/S ________________________and SNDB will ensure that the State Bank of Pakistan is provided necessary access to the documentation and records in relation to the outsourced activities and right to conduct on-site to______________________, if required.

In witnesses hereunder both the parties have set their hands on the day and year above first mentioned.

18. Termination of Agreement by the Bank:

- If the Supplier, in the judgment of the Bank has engaged in corrupt or fraudulent practices in competing for or in executing the Agreement.
- If, as the result of Force Majeure, the Supplier is unable to perform a material portion of the Services for a period of not less than thirty (30) days; and
- If the Bank, in its sole discretion and for any reason whatsoever, decided to terminate this Agreement.
- If issued two (2) warning letter/emails by Sindh Bank Ltd for its unsatisfactory current performance by the Sindh Bank Ltd to the bidder.

Support Escalation Matrix:
For timely addressing of complaints given support escalation matrix will be utilized/followed:-

LEVEL-1	Name/Designation (support staff)	
First complain if the call is not resolved **"within specified response time"** (24 hours)	Landline Phone	
	Email	
	Cell	
LEVEL-2	Name/Designation (Regional Head/Manager/GM)	
Second complain, if the call is attended within **"Specified Response Time" and not attended / or** the problem still unresolved even after complaining at Level-1 (48 hours)	Landline Phone	
	Email	
	Cell	
LEVEL-3	Name/Designation (CEO of the firm)	
Third complain, if the call is attended within **"Specified Response Time" and not attended /or** the problem still unresolved even after complaining at Level-2	Landline Phone	
	Email	
	Cell	
Note: Ensure that no column above is left blank		

Sindh Bank Limited

Registered Address:

Name: ____________________________________

Signature: _________________________________
Title: _____________________________________
Date: _____________________________________

Company Name:

Registered Address:

Name: ____________________________________

Signature: _________________________________
Title: _____________________________________
Date: _____________________________________

Witness:

Name: ____________________________________

Signature: _________________________________
Title: _____________________________________
Date: _____________________________________

Witness:

Name: ____________________________________

Signature: _________________________________
Title: _____________________________________
Date: _____________________________________

ANNEXURE “H”

13. AFFIDAVIT/UNDERTAKING

To be typed on Rs.50/- Stamp Paper

AFFIDAVIT / DECLARATION

(AS REQUIRED BY THE STATE BANK OF PAKISTAN THROUGH BPRD CIRCULAR NO.13, DATED DECEMBER, 11, 2014)

I, __________________ S/o ________________, Proprietor/Authorized Representative/Partner/Director of M/s_______________________, having NTN # __________, holding CNIC # ___________________, do hereby state on solemn affirmation as under:-

1. That the above named firm/company has not been adjudged an insolvent from any Court of law.
2. That no execution of decree or order of any Court remains unsatisfied against the firm/company.
3. That the above named firm/company has not been compounded with its creditors.
4. That my/our firm/company has not been convicted of a financial crime.

That whatever stated above is true and correct as to the best of my knowledge and belief.

City: __________
Dated. _________

DEPONENT
(PROPRIETOR / REPRESENTATIVE / DIRECTOR)

Solemnly affirmed and stated by the above named deponent, personally, before me, on this ______ day of _________ 2020, who has been identified as per his CNIC.

COMMISSIONER FOR TAKING AFFIDAVIT