SNDB/COK/ADMIN/TD/1184/2020
COPY NO: ________________

Sindh Bank Limited

Tender Document

Supply & Installation of Antivirus threat protection Software

This document contains ;33pages

Table of Contents

DEFINITIONS

"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 all documents provided to the interested bidders to facilitate them in preparation of their bids in uniform manner / 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 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 for goods, works and services having the lowest evaluated cost among the substantially responsive bids / 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" means any object of procurement other than goods or works, and includes consultancy services;

"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 FOR BIDS (IFB)

Sindh Bank Limited (SNDB) invites proposal from reputed vendors for Supply & Installation of Computer Servers. Detail of the specifications of related services 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 2013) 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 2013)

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 in drop box at the below mentioned address;

Yours sincerely,

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

INVITATION FOR BIDS (IFB)

Sindh Bank Limited (SNDB) invites proposal from vendors for Supply & Installation of Antivirus Software on need basis. Detail of the specifications of related services to be provided are given in the scope of service in Section [3] hereto.

Bidder will be selected under procedure described in this Tender Document (TD), in accordance with the Sindh Public Procurement Rules 2010 issued thereunder ("**SPPRA**") which can be found at www.pprasindh.gov.pk/. For the purposes of this document, the 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.

This TD 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,

Lt.Col (R). Shahzad Begg
Head of Administration Division
SINDH BANK LIMITED
HEAD OFFICE
Basement-2 Floor, Federation House,
Abdullah Shah Ghazi Road,
Clifton,
Karachi 75600

2. INSTRUCTION TO BIDDERS (ITB)

2.1 Correspondence Address

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

Lt.Col (R).Shahzad Begg
Head of Administration Division
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, 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

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

3.4.1 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.

3.4.2 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)]

3.4.3 Technical Proposal

Bidders are required to submit the Technical Proposal stating a brief description of the bidder's organization outlining their recent experience, the names of Sub-Bidder/Professional Staff who participates during the assignment, the technical approach, sample templates/prototypes of deliver ables, methodology, work plan, organization and staff, including workable suggestions that could improve the quality and effectiveness of the assignment. The firm will be only technically qualified after confirmation of specifications on physical verification of asked items and satisfying of sufficient production mechanism. The date of visit for above inspection by the procurement committee of the bank will be given during process of completing eligibility criteria. After due inspection of requisite items, the bidder will be declared "Qualified" in Technical Qualification Phase.

3.4.4 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 associated with the assignment including remuneration for staff, and reimbursable expenses and such other information as may be specifically requested by SNDB. Alternatively, the bidder may provide his/her/its own list of costs with all items described in the Technical proposal priced separately.

3.4.5 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)]

3.4.6 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].

3.4.7 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)]

3.5 Submission of Bids

3.5.1 Sealing and Marking of Bids

Bid shall comprise a single package containing two separate envelopes. Each envelope shall contain separately the financial proposal and the technical proposal. Envelope shall be marked as "FINANCIAL PROPOSAL" and "TECHNICAL PROPOSAL" in bold and legible letters to avoid confusion.

3.5.2 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)]

3.5.3 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)]

3.5.4 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.

3.5.5 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

3.5.6 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].

3.5.7 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)]

3.5.8 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 during procurement proceedings may lodge a written complaint after the decision causing the grievance has been announced. [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. 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)]

SNDB shall announce its decision as to the grievance within seven (7) days. The decision shall be intimated to the Bidder and the Authority within three (3) working days by SNDB. [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 by a bidder shall no warrant suspension of the procurement proceedings. [SPPRA Rule 31(7)]

A bidder not satisfied with decision of the SNDB complaints' redressal committee may lodge an appeal to the Chief Secretary through the Authority, who shall refer the matter to a review panel in accordance with ITB section [2.5.9]; [SPPRA Rule 31(8)]

A bidder may file an appeal to the Chief Secretary provided; [SPPRA Rule 31(9)]

1. that the bidder has exhausted his complaint to the complaint redressal committee [SPPRA Rule 31(9-a)]; and

2. That he has not withdrawn the bid security deposited by him during the procurement process. [SPPRA Rule 31(9-b)]

The bidder must submit the appeal to the Chief Secretary with the following documents: [SPPRA Rule 31(10)]

1. a letter stating his wish to appeal to the Review Panel and the nature of complaint; [SPPRA Rule 31(10-a)]

2. a copy of the complaint earlier submitted to the complaint redressal committee of the Department and all supporting documents in a sealed envelope; [SPPRA Rule 31(10-b)] and

Upon receipt of an appeal and registration fee, the Chief Secretary shall select a Review Panel to examine the complaint. Simultaneously, the Authority shall inform the bidder and the Head of the concerned Department of the action taken by the Chief Secretary. [SPPRA Rule 31(11)]

On receipt of reference from the Chief Secretary, the Chairperson of the Review Panel shall convene a meeting of the review panel within five working days. [SPPRA Rule 31(12)]

Unless the Review Panel recommends dismissal of the complaint being frivolous, in which case the bidder shall loose the bid security deposited with the SNDB, the Review Panel may: [SPPRA Rule 31(13)]

1. propose rejection of the complaint, stating its reasons; [SPPRA Rule 31(13-a)]

2. state the rules or principles that govern the subject matter of the complaint; [SPPRA Rule 31(13-b)]

3. point out the infirmities and breach of rules and regulations by the procuring agencies; [SPPRA Rule 31(13-c)]

4. suggest annulment in whole or in part of a non-compliant act or decision of a SNDB, other than any act or decision bringing the procurement contract into force; [SPPRA Rule 31(13-d)]

5. if the SNDB is in breach of its obligations under the Act, Rules or Regulations, suggest the payment of compensation by the officer(s) responsible for mis-procurement for cost incurred by the bidder on preparation of bid, including the cost of the complaint registration fee paid by the complainant; [SPPRA Rule 31(13-e)]or

6. Recommends that the procurement proceedings may be terminated, in case the procurement contract has not been signed. [SPPRA Rule 31(13-f)]

It shall be mandatory for both, the complainant and the SNDB to appear before the Review Panel as and when called and produce documents, when so required. The Review Panel shall issue the notice of appearance to the Head of the Department for its service who shall ensure the attendance of the Head of SNDB along with relevant record. In case of failure of Head of SNDB to appear before review panel despite service, the Authority shall bring the matter to the notice of Chief Secretary. In case the complainant fails to appear twice, despite service the reference may be decided ex-parte. The Review Panel shall hear the parties and give its recommendations to the Authority within thirty days of receipt of reference. In case, more time is required, the Review Panel may seek extension from the Chief Secretary through the Authority enumerating the reasons for delay. The Authority shall submit these recommendations to the Chief Secretary who shall decide the appeal keeping in view the recommendations of the Review Panel; Provided that the Chief Secretary may refer the matter back to the Review Panel, if there is some ambiguity or vagueness in the recommendations and a clarification is to be sought. The Review Panel shall clarify the matter within seven calendar days, following which the Chief Secretary would decide the matter; [SPPRA Rule 31(14)]

The decision of the Chief Secretary shall be final and the SNDB shall act upon such findings. After the decision has been issued, the complaint and the decision shall be hoisted by the Authority on its website within three working days; Provided that no information shall be disclosed if its disclosure would be against the public interest or may jeopardize national security. [SPPRA Rule 31(15)]

IMPORTANT

In addition to above it may be noted that no complain will be entertained unless it is forwarded on company's original letter head, bearing complete address, NTN of the company and CNIC of the complainant.

3.5.9 Review Panel

The Authority shall maintain a list of Review Panelists for the purpose of reviewing a bidder's complaint. The Panelist shall be appointed on such terms and conditions as the Authority may from time to time notify with the approval of the Chief Secretary. [SPPRA Rule 32(1)]

The List of Specialists shall be formed from a number [SPPRA Rule 32(2)]

1. persons who have been legal professionals; [SPPRA Rule 32(2-a)]

2. persons who have been senior officers in the service of the Government with experience in the procurement area, [SPPRA Rule 32(2-b)]and

3. Persons from a list of specialists with experience in the relevant field. [SPPRA Rule 32(2-c)]

The Specialists shall be grouped into a number of Review Panels, each with a nominated Chairperson, both as approved by the Chief Secretary. Each panel shall have a minimum of 3 members, one from each of the groups listed in sub rule (2) above and up to 2 co-opted members on a case-by-case basis depending upon the nature of the complaint. [SPPRA Rule 32(3)]

The specialists shall be paid remuneration for their services as determined by the Authority from time to time with the approval of the Chief Secretary. [SPPRA Rule 32(4)]

3.5.10 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)]

3.6 Opening and Evaluation of Bids

3.6.1 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.

3.6.2 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 unless, SNDB may, at its discretion, ask a Bidder for a clarification of bid for evaluation purposes. The request for clarification and the response shall be in writing and no change in the prices or substance of bid shall be sought, offered or permitted. [SPPRA Rule 43]

3.6.3 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 responsive by the Bidder by correction of the nonconformity.

3.6.4 Supplier Eligibility Criteria

All bids shall be evaluated in accordance with the eligibility 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 confirm to the specified requirements.

3.6.5 Eligibility Criteria

S. No.	Requisite	*Evidence required to be attached	Compliance / Proof	
1	Minimum 03 Years in business in the relevant field	Letter of Incorporation / Company Registration Letter / Letter or Declaration of Commencement of Business / NTN. **(attach as Annexure -1)**	Yes	No
2	Turn Over in last 3 Years should be at least 60 million	Audit Report / Tax Return **(attach as Annexure -2)**	Yes	No
3	Registration with Income Tax and Sales Tax	NTN & GST Certificates **(attach as Annexure -3)**	Yes	No
4	Offices in minimum 2 major cities. Office in Karachi is mandatory	Complete address along with PTCL landline numbers **(attach as Annexure -4)**	Yes	No
5	Company must provide a valid Manufacturer Authorization Certificate for Sale/Deal in Pakistan for Antivirus Solution	Manufacturer Authorization Certificate (**Attach as Annexure -5)**	Yes	No
6	The Product / Solution Quoted in the bid must be currently used by at least two Banks in Pakistan other than Sindh Bank.	Attach Purchase Order/ Letter from Manufacturer **(Attach as Annexure -6)**	Yes	No
7	The Products / Solutions Quoted by bidder must be in Gartner's Leaders Quadrant in last two published reports.	(**Attach Report as Annexure -7**)	Yes	No
Qualified / Disqualified				

ELIGIBILTY CRITERIA NOTE

1. There can be 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.
2. 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
3. The bidder may participate with joint venture if required.

MANDATORY

1. GST/Income Tax Registration.
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 on time

QUALIFICATION

1. Attachment of relevant evidence in eligibility criteria is mandatory. In case of non-provision of evidence in any of the requisite, no marks will be awarded (Single Stage- One Envelope Procedure).

DISQUALIFICATION

The bidder will be considered disqualified 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.
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. In Eligibility Criteria, a single non-compliance of a requisite will make the bidder disqualify. (Single Stage-One Envelope Procedure).
10. If during verification process of the cliental list the response by any of the bank is un satisfactory on account of previous performance

3.6.6 Discussions Prior to Evaluation

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

3.7 Award of Contract

3.7.1 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.

3.7.2 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).

3.7.3 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.

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].

3.7.4 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 favor of such person.

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

3.7.5 Performance Security

Within 20 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.

3.7.6 General Conditions of Contract

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

3.7.7 Special Conditions of Contract

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

3.7.8 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]

3.7.9 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"]*

3.7.10 SCOPE OF WORK / TECHNICAL SPECIFICATION

Proposed solution must have following features / specification

Quantity 2000 clients

Scope OF Work/Technical Requirement		Compliance (Yes/No)	Comments
Anti-Virus Protection	Proposed solution must have cloud based management server and interface for endpoints		
	The proposed solution must include signature based detection with behaviour monitoring and machine learning		
	Proposed endpoint solution must have Machine Learning Technology		
	The solution must have technologies to detect, stop and restore encrypted files from ransomware		
	Antivirus protection software for Windows workstations including Windows XP,7,8 and 10		
	Antivirus protection software for Windows Server 2003, 2008, 2012, 2016 and 2019 file servers		
	Antivirus solution must provide following features		
	· Anti-Malware		
	· Protection Against Browser Exploits		
	· Anti-Virus		
	· Anti-Trojan		
	· Anti-Spyware		
	· Anti-Worm		
	· Anti-Root kit		
	· Anti-Ransomware		
	· WEB/URL Filtering		
	· Device Control		
	· Memory exploit detection		
	· ML-driven threat protection		
	· Integration Endpoint Detection and Response “EDR”, Anti-APT solution,		
	Proposed solution must provide security for these components:		
	· Files		
	· Web		
	· HIPS or Vulnerability Protection feature		
	· Network based suspicious connection		
	· Behavior Detection		
	· Exploit Prevention		
	following components in a single agent installed on the endpoint:		
	· Application, Web reputation and Device control		
	· HIPS and Firewall		
	Proposed endpoint solution must allow the following:		

	· Manual scanning		
	· On access scanning		
	· On demand scanning		
	· Compressed File Scanning		
	· Script blocking and scanning		
	· Removable drive scanning upon connection with system		
	Ability to detect untrusted hosts and block upon detection of encryption like activities (renaming of extensions) on the server shared resources with a feature like anti-cryptor		
	Pre-execution detection and blocking of new and evolving threats (advanced machine learning, sandboxing to detect malware, and suspicious file behavioural monitoring and blocking), and signature-based methods		
	Protect against CnC connections		
	Terminate memory resident virus processes		
	web protection to prevent access to malicious websites		
	Solution Must have host-based firewall		
	Intrusion Prevention System (IPS)/s that show CVE on each endpoint that are being protected		
	Application control feature to implement blacklisting or whitelisting or lock-down		
	Should be able to detect removable devices on Linux		
	Should be able to detect when a software is installed or uninstalled on Unix		
	Cloud Based Sandbox Integration with Endpoints		
	Sandbox integration must help provide protection against unknown files which are malicious in nature.		
Forensic Information & EDR	Able to View execution event graphs or RCA to gain a clear understanding of all events caused by malware.		
	EDR agent must have integration with Endpoint Protection application (Single agent)		
	EDR solution must provide means of isolating machine from the rest of the network		
	EDR solution must provide means of remote remediation via agent (file block, process kill, preventing particular files from running/opening, etc.)		
	Solution should provide RCA for monitoring and visualization efficient analysis		
	Solution should provide the ability to record and analyze endpoint behavior to identify Advanced Attack Techniques and map to MITRE tactics and techniques		
	Sandbox Integration with endpoint should be included in endpoint offering		
	Solution should provide Protection from Zero Day with Sandboxing		
	Solution should deliver powerful IT security operations hygiene and threat hunting for both IT admins and security analysts		

Solution Interface	The program interface of all antivirus products, including management tools, should be in English.		
	All antivirus products, including management tools, should have a context-dependent help system in English.		
	Antivirus solution must be capable to centrally administrate unmanaged/unassigned and managed/assigned computers.		
	Centralized collection of statistical information, creation and viewing of reports		
Centralized Updating	Centralized, automatic and real time update of antivirus protection software and antivirus databases		
	Should be able to get updates on Peer to Peer basis, Repository, Internet.		
Administration Console	The proposed solution must have administration web console that should be accessible from most common browsers and is accessible anytime, anywhere and from any device with the supported browser.		
Ease of management and reporting	The solution should have easy-to-use management tools and reporting feature.		
	Reports can be Scheduled to be sent to specific Email Addresses		
	Reports can be exported in any one of formats pdf, excel		
Application Control	The solution must include Application Control tools that give administrators granular control over which applications are permitted to run on the corporate network – and how an application is allowed to run.		
	Proposed solution must provide application control feature to implement blacklisting or whitelisting or lock-down		
	Able to block Legacy based (Desktop) Applications like Hotspot Shield, UltraSurf etc.		
Device Control	The solution must include Device Control features that help you to control the use of removable and plug and play devices and prevent unauthorised devices compromising security. The solution's Device Control feature should include the following features:		
	The solution must be able to restrict device access on endpoints by assigning rights to read, read / write, write and deny access to USB drives.		
	CD ROM blocking		
	Network Shares		
	Proposed solution must be able to block the usage of USB storage devices or only allow access to whitelisted devices and allow read/write access by domain users to reduce data theft		

Encryption	The proposed solution must support encryption on multiple levels: • Full disk encryption – including system disk • File and Folder encryption • Removable media encryption		
	The proposed solution's encryption module should be separately managed to avoid single point of failure on all computers with ability to enforce encryption policies and modify/stop encryption settings		
	The proposed solution should have the ability to centrally monitor encryption status and generate reports on encrypted computers/devices		
	The proposed solution must also provide management for BitLocker		
Data Leakage Prevention or Equivalent	Proposed Solution should provide data leakage protection on Web, Email, sysmtems and Application channel		
	The proposed solution should have data discovery capability on endpoints		
	The proposed solution should protect against data leaks via USB drives and other channels based on specified sensitive content		
	The proposed solution should be able to stop data leakage on Web and Email and via printer		
	The proposed solution must have capability to protect data leakage on keywords		
	The proposed solution must have capability to protect data leakage on expressions		
	The proposed solution must have capability to protect data on the basis of file type		
	The proposed solution must support user justification option when violating the DLP policies		
	The proposed solution must have cpability to block copy/paste feature for the protected data		
	The proposed solution must have multiple mode of data Leakage like block & pass.		
	The proposed solution must have capability to block print-screen function		
Mail clients software compatibility	The proposed solution be installed on MS Exchange Server and able to scan internal emails.		
	Able to Remove Malware, Mailbox Level		
	The solution must perform real-time search and removal malicious content in the flow of incoming and outgoing mail messages, including attachments;		
	Solution should provide DLP feature to reduce the risk of unsolicited data exfiltration		
	The solution must detect malicious and phishing links in the message body		
	The solution must have heuristic detection methods		

	Solution should provide protection from Business Email Compromise and other advanced email threats.		
	Solution should provide protection from embedding malicious scripts into Office files is a popular technique used by extremely dangerous specimen.		
	The solution must be able to add warnings about unsafe attachments to incoming messages in the subject line		
	The solution must process mail messages according to the rules specified for groups of senders and recipients		
	The proposed solution must detect social engineering attacks		
	The proposed solution must provide the ability to examine the message contents to determine whether the message contains inappropriate content		
	The proposed solution must allow to filter senders of incoming email messages.		
	The proposed solution must include integrated DLP feature to prevent data loss by monitoring outbound email traffic		
	The proposed solution must provide integration with Syslog or SIEM server for centralized log storage and monitoring.		
	Administrator must be able to review and manually delete or deliver messages held in quarantine on the Administrator Console.		
	The proposed solution be installed on MS Exchange Server and able to scan internal emails for hateful content		
	The proposed solution must support Exchange Server 2013, 2016 and 2019		
	The proposed solution must support SMTP scanning		
	The proposed solution must support file type recognition to detect falsely labelled files		
	The proposed solution must detect document exploits and other threats used in advanced attacks		
	The proposed solution must support scanning for mailbox		
	The proposed solution must support content filtering rules		
	The proposed solution must support data loss prevention to block sensitive data		
	The proposed solution must provide anti-spam capability on MS Exchange		
	The proposed solution must include search and delete feature to delete unwanted content from email.		
Cloud Email Gateway	The proposed solution must be a cloud-based solution that provide protection to stop ransomware, spam and phishing.		
	Proposed solution must provide advanced protection for Gmail, google, MS Server, MS office 365 and other cloud or on-premises email solutions		
	The proposed must stop new and sophisticated threats such as ransomware, spear phishing, and business email compromise with the most effective and accurate email security		

	Proposed solution must uncovers targeted and advanced attacks by executing unknown files in cloud sandbox integrated with Email Security		
	Solution should provide protection from embedding malicious scripts into Office files is a popular technique used by extremely dangerous specimen.		
	Solution should simplifies the process of achieving and maintaining sender authentication enforcement by using automation to support various standards (e.g. DMARC, DKIM, SPF).		
	The proposed solution must deliver email continuity against planned or unplanned downtime events, which allows end users to continue sending and receiving email messages for up-to 10 days in the event of an outage with the capability available in the proposed solution itself		
	The proposed solution must have sandbox analysis in the cloud sandbox to analyze suspicious URLs embedded in email body.		
	The proposed solution must have sandbox analysis in the cloud sandbox to analyze suspicious URLs embedded in email attachments.		
	The proposed solution based on the customer defined passwords submitted, must be able to extract encrypted archive files and analyse encrypted files in email messages to investigate any malicious or suspicious content or URLs in those messages		
	The proposed solution must include integrated DLP feature to prevent data loss by monitoring outbound email traffic		
	The proposed solution must provide Identity Based Email Encryption.		
	The proposed solution must support following directory types: MS AD Global Catalog, MS 365/Azure Active Directory, Open LDAP and Microsoft Active Directory		
Web Security Gateway (Hybrid Deployment)	The proposed solution must include cloud proxy for roaming users and on-premises software appliance for local enterprise users with centralized cloud management		
	Block malicious and phishing websites		
	The solution must include flexible Web Control / Filtering functionality which allows administrators to prevent the corporate network from being used to access inappropriate websites.		
	Solution should control user access to internet resources based on the website categories and types of content defined by the manufacturer of the protection product.		
	The centralized web control / filtering feature must make it easy to monitor and filter each employee's web browser usage.		
	The proposed solution must include cloud proxy for roaming users and on-premises software appliance for local enterprise users with centralized cloud management		
	The solution should provide multi-layered gateway-level protection against the latest web-based threats		

	Perform anti-virus scanning of objects transferred through the proxy server.		
	Detect and blockmalware in all types of files		
	Block malicious and phishing websites.		
	Monitor and protect SSL-encrypted network traffic		
	Control user access to internet resources based on the website categories and types of content defined by the manufacturer of the protection product.		
	Support URL masks and regular expressions as filters.		
	Ability to decrypt HTTPS traffic using a self-signed or corporate certificate.		
	Ability to set exclusions in decryption rules.		
	Integrate with Microsoft Active Directory to assign roles to management console users.		
	Provide support for NTLM and Kerberos authentication for the single sign-on service.		
	Solution should block infections before they can reach your endpoints		
	The proposed solution must allow protecting of iOS-based and Android-based mobile devices		
	The proposed solution must monitor and analyse web traffic status and network threats by using the dashboard, log and report features		
	The proposed solution must assign suitable bandwidth resources for critical traffic to control communications		
	The proposed solution must decrypt and inspect encrypted content		
	The proposed solution must facilitate a more user friendly experience by providing multiple types of event notifications, alerts, and messages to users and administrators		
	The proposed solution must support dynamic URL categorization technology to perform real time categorization of the website based on the website content and HTTP URL		
	The proposed solution must provide machine learning feature for unknown malware detection		
	The proposed solution must support authentication with on-premises AD, Microsoft® AD, Okta and ADFS		
	Solution should detect advanced attacks		
	Investigate incidents by searching and viewing events.		
Server Security Requirement	The solution must provide single dashboard for physical, virtual and cloud servers.		
	Proposed solution must have support for following OS Windows, Linux		
	Proposed solution must have support for Server 2003 and Server 2008, Server 2012, 2016 & 2019		

	Provides layered defense against advanced attacks and provide protection/Virtual Security Layered against vulnerabilities on OS level and application level		
	Should be able to provide virtual security layered against WebSphere Application Server vulnerabilities		
	Should be able to provide virtual security layered against Oracle Web Logic Vulnerbilites		
	Should be able to identify use of PSEXEC tool through SMB share		
	Should be able to detect and alert if executable file is being uploaded on a SMB share		
	Should be able to detect and alert batch file upload on network share		
	Should be able to identify and alert on suspicious (RDP) possible attempt of brute force		
	Should be able to prevent access to administration share		
	Should be able to detect OneDrive, Dropbox, BOX traffic		
	Should be able to detect download of a file over FTP		
	Should be able to detect traffic remote applications like VNC and TeamViewer		
	The proposed solution must provide firewall feature on Windows, Linux.		
	The proposed solution must have application control feature to quickly identify new suspicious files.		
	The proposed solution must provide IPS feature on Windows, Linux.		
	The proposed solution must be able to detect and alert on administrator log-ins on servers		
	The proposed solution must be able to alert when log file is cleared (e.g. Windows Event Logs)		
	The proposed solution must be able to detect PowerShell command execution		
	Should be able to detect ftp event on Windows		
	Should be able to provide lock-down ability (to block all new executable) if needed on Linux		
	Should be able to provide information on the user and process associated with launching of executable		
	Should be able to provide a way to block suspicious list of hashes on Linux		
	Should be able to list down the vulnerabilities being protected with relevant CVE and CVSS score		
	Should be able to provide a mechanism to block suspicious web traffic on servers		
File Integrity Monitoring (FIM) for Servers	Proposed solution must have file integrity monitoring on Windows, Linux, Servers Platforms		
	Solution should keep track of changes in file data with an interactive dashboard		

	Efficiently track changes to files in environments of all sizes		
	Must be able to monitor critical OS and application.		
	Solution must detect and alert on changes to key files, folders, and registry settings		
	Solution should alerts when unusual file modifications occur		
	Events can be triggered for Renaming of files or directories		
	Must provide agent-less recommendation or baseline scan		
	Should be able to detect hosts file modification on Windows		
	Should be able to detect change in the attribute Permissions of any log file under /var/log path		
	Should be able to alert when command history is cleared		
	Should be able to detect installation of root certificate		
	Should be able to identify create and delete activity of users and groups		
	Should be able to detect when task scheduler entries are modified		
	Should be able to detect when Windows startup programs are modified		
Network APT Solution with Sandbox	The proposed solution must come with dedicated hardware to avoid sizing and performance complications. In case of Software Appliance, Vendor should quote/inlcude required Hardware		
	Security vendor should have a platform to address APT and Advanced Malware across network proactively		
	Solution should have behavior detection capabilities and analyzes traffic and objects		
	Virtual Execution must be on premise as network appliances and not in the cloud		
	The current requirement of Sindh Bank is to inspect up-to 1G of traffic irrespective of number of users involved		
	The proposed solution must support protocols including SMB for lateral movement detection		
	The proposed solution must have the ability to create customized sandbox images for virtual execution based on the Sindh Bank environment		
	The solution must be able to detect and report malware downloaded		
	The sandbox solution must not be detectable by malware in order to avoid evasion		
	The solution must have ability to simulate end user actions in order to force the execution of malware that rely on triggers from and end user, like a mouse click		
	The solution must provide the full detailed malware analysis report for the malware executed in sandbox		
	The solution must Supports custom YARA rule importation		

	Solution should perform dynamic real-time analysis of advanced malware on the appliance itself to confirm true zero-day and targeted attacks		
	The solution should provide network exploit detection		
	The solution should provide document exploit detection		
	The solution should provide feature to analyze scripts		
	The solution should be able to handle evasion tactics (Anti-VM, Anti-Sandboxing and Anti-Debugging)		
	Solution should have the ability to remain completely invisible to both the end user as well as the attacking website		
	Solution should support the following Windows operating systems for sandbox: MS Windows XP, 7, 8, 8.1 10,		
	Solution should support the following Windows operating systems for sandbox: Windows Server 2003, 2003 R2, Windows Server 2008, 2008 R2, Windows Server 2012/2012 R2, Windows Server 2016, Windows Server 2019		
	Solution should be able to detect rootkits		
	Solution should be able to handle DLL injections		
	The solution must be able to accurately identify malware and maintain a very low false-positive rate.		
	The solution must allow the administrator to associate file extensions to the applications that will run the files in the sandbox.		
	Solution should have the ability to display the geo-location of the remote command and control server(s) when possible		
	Solution should have the ability to report the Source, Destination, Detection Name, Detection Severity and Protocol		
	Solution should detect potential malicious network traffic, such as DNS queries to Botnet C&Cs		
	Solution should monitor SMTP Traffic		
	The solution should be able to integrate with SIEM		
Systems Management, vulnerability and patch management or Equivalent	Proposed solution should include features to manage the computers remotely like remote installation of third party software, removal of unauthorized software, reports on existing software and hardware		
	Proposed solution should include patch management capabilities for Windows operating systems and installed third-party applications		
	The proposed solution's patch management functionality should be fully automated with ability to detect, download and push missing patches		
	The proposed solution must provide facility to select which patches to be downloaded/pushed to endpoints based on their criticality		
	The proposed solution should have the capability of pushing specific patches based on criticality or severity		

	Proposed solution management server must have ability to be configured as Updates source for Microsoft Updates and third-party applications.		
	The proposed solution should have the capability to automatically identify missing patches from individual		
	The proposed solution should provide the facility to manage missing patches for operating system and third-party application separately		
	Proposed solution must support Wake-on LAN and UEFI		
	Proposed solution must have the ability to be configured / assigned as an update source for Microsoft and third-party updates		
	Proposed solution must have the ability to remotely push/deploy EXE, MSI, bat, cmd, MSP files and allow the administrator define the command line parameter for the remote installation.		
	Suggest solution must be able to administer third party application licenses. And notify the violations.		

Note:

1. Installation of software on all pc/laptops/servers will be carried out by bidder.
2. Bidder will be responsible for smooth/ error free running of the solution and an integrated / unified security management solution for efficient & secure operation.
3. Resident engineer shall be dedicated to the bank to resolve the day by day support issues and deployment of the project without any additional cost to the bank.
4. Un-installation of existing/previously installed antivirus software on pc/laptops/servers will be carried out by bidder.
5. Bidder must provide 24*7 support including public holidays.
6. Bidder will be responsible to arrange recourses for deployment of software on all pc/laptops/servers.
7. Bidder will responsible to provide training to IT support staff.
8. Bidder will ensure that during antivirus scanning task system pc/laptops/servers performance not be effected and end users will perform their routine task smoothly.
9. Bidder will be responsible to create centralized management server at Primary Site as well as DR Site.
10. Bidder will be responsible to resolve all within four hours.
11. Bidder will share escalation matrix with Sindh Bank Ltd.
12. Bidder will provide operational manual of proposed solution.
13. Software upgrade support must be provided free of cost
14. Delivery Time: Within 2 weeks.
15. The Bidder must mention renewal fee in bid to get upgrade for subsequent years
16. Contract agreement is extendable / renewable up to 3 years only on mutual understanding on same terms & conditions and rates.

4 FINANCIAL PROPOSAL

PRICE SCHEDULE

(Applicable for the year 2020-2021)

Name of Bidder ____

S.No	Item	Total Amount
01	Anti Virus Software with 2000 clients (With Media Kit)	
	*Total Amount	

**This Total Amount will be taken as the financial bid offered by the vendor.*

Note

1. 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.
2. If the item is not provide/installed on due date (date given on supply order) a fine of Rs.500/-per day will be deduced from the bill.
3. The cost must include all taxes, stamp duty (as applicable under Stamp Act 1989) duly stamped on the contract agreement, installation, commissioning, transportation and labour charges.
4. No advance payment for the supply of equipment will be made, bills are only be processed for necessary payment on receipt of certificate of delivery/satisfaction from the concerned officer.
5. Calculation of bid security. 5% of the *(Total Amount) will be submitted with the tender document as bid security in shape of Pay Order/Demand Draft /Bank Guarantee in favour of Sindh Bank Ltd.
6. The successful bidder will be the one whose total sum of cost is the lowest. As it is package tender, so no partial lowest cost will be considered for award of any work.
7. The tender will be considered cancelled if the contract agreement/performance security after due signature are not submitted with Admin Office after 5 days of completion of bid evaluation report hoisting period (7 days) on SPPRA website.
8. The Tender will stand cancelled if the item are not supply/installed within 8 weeks of issue of supply order.
9. In case financial bids are the same, the successful bidder will be the one who has highest turnover of the two.
10. If the obligation of warranty period are not met or delayed, the repair etc. requirement on this account will be carried out by the bank & the billed amount will be deducted from the performance security/ upcoming payment due to supplier. Risk & subsequent cost to this effect if any will be liability of the vendor and any subsequent expenses on the equipment will also be borne by the supplier.
11. Qualified company will also be bound to sign a bond/undertaking that in case of any observation arising in respect of quality of the equipment 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.
12. All terms & conditions of the Contract Agreement (Annexure “G”) are part of tender document.
13. The tender will stand cancelled if any of the given condition of the tender is not met in strictly as per the requisite of the tender document.
14. Pre Bid Meeting: Within one week (For Any Clarification)
15. Note. There can be 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 website regularly.
16. Payment will be made in Pak Rupee.

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.

"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 5.1.17 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.

5.1.9.1 No Breach of Contract

The failure of a Party to fulfill 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.

5.1.9.2 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.

5.1.10 Termination

5.1.10.1 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.

5.1.10.2 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.

5.1.10.3 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), and (f) 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.

5.1.11 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.

5.1.12 Settlement of Disputes

5.1.12.1 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.

5.1.12.2 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.

5.1.13 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.

5.1.14 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.

5.1.14.1 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.

5.1.14.2 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.

5.1 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 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 [IT SHOULD BE SPECIFIC TO EACH CONTRACT AND WILL HAVE TO BE TAILORED SEPARTELY FOR EACH TENDER DOCUMENT]

Dated: ___________, 2020

To,

Head of Administration Division
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 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 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:

Name & Address of Agent	Amount and Currency
________________________	____________________
________________________	____________________

(If none, State none)

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

Dated this ___________ day of _________ 201____.

____________________ ______________________

[Signature] *[In the Capacity of]*

Duly authorized to sign Bid for and on behalf of ____________________________

Annexure "B"

7. BID SECURITY FORM

Whereas [name of the Bidder] has submitted its bid dated [date of submission of bid] for ____.

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 SNDB (hereinafter called "the Purchaser") in the sum of 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 SNDB 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 Administration Division
SINDH BANK LIMITED
CAMP OFFICE
3rd 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.

Signature and Seal of the Guarantors

Name of Bank

Address

Date

Annexure "D"

9. INTERGRITY 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 Availability, Submission & Opening of Bids

Please refer to Notification Advertisement on the subject matter.

11. Form of Contract Annexure "F"

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 fulfill 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	Company Name:
Registered Address:	Registered Address:
Name: ___________________________________	Name: ___________________________________
Signature: ________________________________	Signature: ________________________________
Title: ____________________________________	Title: ____________________________________
Date: ____________________________________	Date: ____________________________________

ANNEXURE- G

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 Equipments for the BANK of total sum Amounting Rs. ____________ .

Detail of Equipment is as follows.

S.No	Product	Quantity	Unit Price PKR	Total Price (PKR) Including All Taxes
1				

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 1- year 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 8 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.

In addition the Bank will have the option to cancel the order and offer the same to the next lowest bidder.

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 equipments in good and sound condition.

5. The warranty of the equipment is 3- years 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 equipment to the vendor site. In case however if any portion of equipment required to be shifted to vendor's site, vendor will provide equivalent backup during the warranty period.

7. Vendor should maintain adequate inventory of the parts so that the replacement is available within 24 hours, if any fault arises in the equipment during the warranty period. In case the effected part is not available, then the vendor will provide backup equipment of the same product or better till the resolution of the fault, without any extra cost to the Bank.
If problem does not resolve within 10 days and suitable backup is also not provided then Bank will have the right to get it resolve its own from the open market and charge the actual cost to the vendor without any further referring to the vendor.

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 equipment 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 the Bank will be the final and legally binding on the vendor.

11. Proportionate payments against supply of equipment will be made within Thirty days from the equipment 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.

15. The term of this agreement shall be for a period of one year, commencing from the date of signing of this agreement. Expendable upto 3-years.

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

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		

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

Sindh Bank Limited

Registered Address:

Name: ___________________________________

Signature: ________________________________
Title: ____________________________________
Date: ____________________________________

Witness:

Name: ___________________________________

Signature: ________________________________
Title: ____________________________________
Date: ____________________________________

Company Name:

Registered Address:

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 _________ 201 , who has been identified as per his CNIC.

COMMISSIONER FOR TAKING AFFIDAVIT