SNDB/COK/ADMIN/TD/1173/2020
COPY NO: _____

Sindh Bank Limited

Tender Document

Procurement of SIEM/Log Management System

This document contains ;59 pages

Table of Contents

I. 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 Procurement of SIEM/Log Management System on need basis. Detail of the specifications of related services to be provided are given in the scope of work/technical specifications 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 Amended 2017, 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 2017.

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 in drop box at the below mentioned address;

Yours sincerely,

Information Technology Department SINDH BANK
LIMITED

HEAD OFFICE
Basement-2 Floor, Federation House, Abdullah Shah Ghazi Road,
Clifton, Karachi 75600

2 INSTRUCTION TO BIDDERS (ITB)

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

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

2.1 Correspondence Address

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

Information Technology Department
SINDH BANK LIMITED
HEAD OFFICE
3rd Floor, Federation House,
Abdullah Shah Ghazi Road,
Clifton,
Karachi 75600
Tel: 021-35829394/35829403

2.2 Eligible Bidders

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

2.3 Corrupt Practice

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

2. SNDB will reject a proposal for award, if it determines that the Bidder recommended for award was engaged in any corrupt or has been blacklisted under the Sindh Public Procurement Rules 2010 Amended 2017, in competing for the contract in question.

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

2.4 Preparation of Bids

2.4.1 Bidding Process

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

2.4.2 Cost of Bidding

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

2.4.3 Language of Bid

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

2.4.4 Technical Proposal

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

2.4.5 Financial Proposal

The Financial Proposal shall be prepared using the standard form attached, duly signed by the authorized representative of the Bidder. It should list all costs inclusive taxes associated with the assignment including remuneration for staff, and reimbursable expenses and such other information as may be specifically requested by SNDB.

2.4.6 Bid Currencies

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

2.4.7 Bid Security

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

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

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

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

The bid security shall be forfeited:

- If a Bidder withdraws its bid during the period of its validity specified by the Bidder on the Bid Form; or
- In the case of a successful Bidder, if the Bidder fails to;

1. Sign the contract in accordance with ITB Section [2.7.4]; or
2. Furnish performance security in accordance with ITB Section [2.7.5].

2.4.8 Bid Validity

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

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

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

2.5 Submission of Bids

2.5.1 Sealing and Marking of Bids

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

Technical Proposal may be submitted in duplicate (one original and one copy). In case any conflict, the original bid will be considered as final.

2.5.2 Response Time

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

2.5.3 Extension of Time Period for Submission of Bids

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

3. 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)]

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

2.5.4 Clarification of Bidding Documents

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

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

2.5.5 Late Bids

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

2.5.6 Withdrawal of Bids

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

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

2.5.7 Cancellation of Bidding Process

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

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

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

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

2.5.8 Mechanism for Redressal of Grievances

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

Any bidder being aggrieved by any act or decision of the SNDB during procurement proceedings may lodge a written complaint after the decision

causing the grievance has been announced. [SPPRA Rule 31(3)]

/ Any bidder being aggrieved by any act or decision of the SNDB after the issuance of notice inviting tender may lodge a written complaint.

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 not warrant suspension of the procurement proceedings. [SPPRA Rule 31(7)]. Provided that in case of failure of the complaint Redressal Committee to decide the complaint; SNDB shall not award the contract.

IMPORTANT

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

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

2.5.9 Review Committee

A bidder not satisfied with decision of the procuring agency's complaints redressal committee may lodge an appeal to the Review Committee; provided that he has not withdrawn the bid security, if any, deposited by him. [SPPRA Rule 32 (1)].
The bidder shall submit the following documents to the Review Committee: [SPPRA Rule 32 (5)].
(a) A letter stating his wish to appeal to the Review Committee and nature of complaint; [SPPRA Rule 32 (5-a)].
(b) A copy of the complaint earlier submitted to the complaint redressal committee of the department; [SPPRA Rule 32 (5-b)].
(c) Copy of the decision of Procuring Agency / Complaint Redressal Committee. [SPPRA Rule 32 (5-c)].

On receipt of appeal, the Chairperson shall convene a meeting of the Review Committee within seven working days; [SPPRA Rule 32 (6)].
It shall be mandatory for the appellant and the Head of procuring agency or his nominee not below the rank of BS-19 to appear before the Review Committee as and when called and produce documents, if required; [SPPRA Rule 32 (8)].
In case the appellant fails to appear twice despite the service of notice of appearance, the appeal may be decided ex-parte; [SPPRA Rule 32 (9)].
The Review Committee shall hear the parties and announce its decision within ten working days of submission of appeal; [SPPRA Rule 32 (10)].
The decision of Review Committee shall be final and binding upon the procuring agency. After the decision has been announced, the appeal and decision thereof shall be hoisted by the Authority on its website; [SPPRA Rule 32 (11)]

2.5.10 Matters not subject to Appeal or Review

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

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

2.6 Opening and Evaluation of Bids

2.6.1 Opening of Bids by SNDB

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

2.6.2 Clarification of Bids

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

2.6.3 Preliminary Examination

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

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

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

2.6.4 Supplier Evaluation Criteria

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

2.6.5 Eligibility Criteria

SNDB shall evaluate Technical Proposals using the following eligibility/technical 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 50 million	Audit Report / Tax Return **(attach as Annexure "2")**	**Yes**	**No**
3	Registration with Income Tax , SRB and Sales Tax	NTN , SRB & GST Certificates **(attach as Annexure "3")**	**Yes**	**No**
4	The proposed solution / product in the bid must be currently used by atleast three Bank in Pakistan other than Sindh Bank	Attach Documentary Evidence/Certificate **(attach as Annexure "4")**	**Yes**	**No**
5	The proposed solution / product must be currently deployed by the vendor atleast in two Bank in Pakistan other than Sindh Bank	Attach Documentary Evidence/Certificate **(attach as Annexure "5")**	**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

MANDATORY

1. GST/Income Tax Registration/Sindh Revenue Board.
2. Attachment of Affidavit (specimen attached as Annexure "H") on stamp paper from the owner of the company.
3. Attachment of Annexure "A" (With Financial Proposal) & Annexure "B" (With Financial Proposal if Bank Guarantee is going to be submitted as Bid Security).
4. Writing of tender reference as given in the NIT on the Envelop, carrying tender document is must or the bank will not be responsible if the documents are not received by the Procurement Committee on time

2.6.6 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

2.6.7 Discussions Prior to Evaluation

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

2.7 Award of Contract

2.7.1 Award Criteria

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

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

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

2.7.3 Notification of Award

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

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

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

2.7.4 Signing of Contract

Within 10 Days from the date of notification of award, the successful bidder shall furnish to SNDB particulars of the person who would sign the contract on behalf of the successful bidder along with an original power of attorney executed in favour of such person.
The Contract shall be signed by the parties at Central Office SNDB, Karachi, within 10 Days of letter of acceptance date and furnishing the requisite performance security.

2.7.5 Performance Security

Within 7 DAYS of receipt of the notification of award from SNDB, the successful Bidder shall furnish to SNDB the Performance Security equals to 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,the date of successful completion of the Supplier's performance obligation under the Contract.

2.7.6 General Conditions of Contract

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

2.7.7 Special Conditions of Contract

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

2.7.8 Integrity Pact

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

2.7.9 Non Disclosure Agreement

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

3 SCOPE OF WORK / TECHNICAL SPECIFICATION

Technical Specification

3.1 Objective:

- The proposed system is one of ways to maintain situational awareness and security posture of organizational identified critical automated systems and infrastructure components in support of the Risk Management.
- The proposed system will increase the efficiency of the cyber security team, Information technology and systems operation teams besides fostering a broader awareness and a culture of IT Security and risk management.
- Institution's risk posture identification, reduction and improvement in Banking and Enterprise systems and associated critical Infrastructure components.
- The system will be served as a nerve center towards establishing a Cyber Security Operation Center (SOC).
- The proposed system is an actionable, preemptive, and enabling approach and measures through an independent and unbiased entity.
- The system provides a centralized platform and real-time actionable and comprehensive security insight and contextual information for managing cyber risks and threats from detection and protection through remediation.
- The proposed system provide real-time centralized repository or platform of monitoring and detection of cyber security events, logs, traces, footprints left by hackers / malicious insiders and privileged users activities and subsequent reporting of cyber threats, attacks and breaches to IT Operation teams and Management for mitigation and/or elimination.
- The proposed system will provide insight in Policies, Controls and Threats compliance. It will provide a controlled IT environment in terms of change and configuration management.

3.2 Project Management

Sr. No.	Approach
1.	As part of the bid submission, the bidder must include the complete high-level and detailed tentative project plan clearly highlighting the milestones – Schedule, Timelines, Methodology, Roles and responsibility related to different activities like, but not limited to, Ordering, Delivery, Sizing, Designing, Training, Integration, Configuration, Implementation, Customization, Testing, Optimization, Archiving, Maintenance Support and Services of the proposed solution.
2.	Once the contract is awarded to the successful bidder, the kick off meeting(s) will be conducted in the bank premises for the actual project plan with the successful bidder
3.	After the notification of award to the successful bidder, will provide the name of Project Team Lead and team resources those will be assigned to SNDB Security Intelligence and Threat Management System implementation and roll-out.

4.	Successful bidder must provide detailed CVs of project resources assigned to SNDB Security Intelligence and Threat Management System implementation and roll-out.
5.	The successful bidder nominated Project Team Lead/Manager will be responsible for handling the communications and coordination with their management, technical team and SNDB. Project Team Lead/Manager will also be responsible for providing the project status on regular basis.
6.	Change or removal of any resource from the Project team during execution of the project will be subject to SNDB approval. The supplier will submit the CV of the proposed resource(s) for SNDB review. In case of any change in the supplier's allocated Project Team Lead/Manager or team member, the supplier will provide the resource immediately of equivalent or higher qualification and experience.
7.	SNDB may request to change any project resource, in case their performance is not up to the mark or as per institution satisfaction.
8.	Project Supplier may engage foreign / local experts/consultants should they feel it is necessary for the project at their own cost.
9.	The Project Supplier may perform the implementation through Professional Implementation Services from the principal/OEM effectively and efficiently.
10.	The Project Supplier will also provide the Post Implementation Optimization, customization, upgrade, health-check services of the system and also assist the SNDB till acceptance of the system.
11.	During the project, the supplier should provide information on help desk support levels arrangements, End of Life and End of Support information for the proposed product/solution, software support, release management, on-site and remote support, on-line services self-diagnostics tools, ticket and case escalation etc.
12.	Project supplier support and guidance for the IT/Cyber security operation center (IT/Cy.SOC) to SNDB including but not limited to SOC requirement analysis/processes, design/strategy, Implementation of additional tools to supplement SOC capability and threat intelligence, incident handling, investigation, forensics and response.

3.3 Project Timeline

The targeted Project Timeline is 6 (Six) months or earlier including the delivery, implementation and operational acceptance from the date of signing of contract.

3.3.1 Delivery

Delivery will be considered accomplished when all the software and allied components have been delivered at designated location and installed in accordance to the contract.

All related hardware, storage, software licensing shall be in the name of SNDB – registered with OEM where applicable.

3.3.2 Implementation / Deployment

The supplier shall, with due care, diligence and attention implement and deploy the complete system with warranty and technical support and professional services according to the requirements and maximum satisfaction of the SNDB by assigning properly qualified and competent personnel having related product maintenance experience and exercising all reasonable means required in ensuring quality services in accordance with this Agreement.
The On-premises implementation phase / criteria must include but not limited to:

Sr. No.	Implementation phase / criteria
1.	Installation and configuration of server/appliance, applications and associated modules etc.
2.	OEM based accredited training for the system/solution operation management, security analyst and Cyber SOC management
3.	Network configurations - dedicated high speed network interfaces for load balancing (i) system administration, (ii) logs and events push/pull and collection, (iii) network flows.
4.	Integration and configuration of agent and agentless log sources as per requirements to achieve the objectives.
5.	Integration and configuration of network flows (Information will be provided at this stage of implementation)

6.	Normalization/Parsing of logs/events
7.	Aggregation and correlation for analytic of logs/events
8.	Centralized (Security Operation) and specialized dashboards (Networks, Databases, Hosting Systems, Applications, Privileged Users Activity, Executive Management, Audit & Compliance, System Health Check, Work flows/Ticket escalation, progress, status etc.) development and customization
9.	Use / Misuse cases development and deployment, alarms, alerts and reporting
10.	Integration of open source or proprietary threat intelligence feeds
11.	Ticket escalation/workflow configuration to support incident response
12.	Integration and configuration with Vulnerability and Patch management system if required
13.	Testing and Optimization (Health Check)
14.	The implementation, integration, configuration, customization and service related tasks done by supplier will be checked and validated by OEM professional services

The supplier backed by OEM must provide the **best technical and security analytical implementation solution** effective for SNDB IT security until operational acceptance

3.4 Training

SNDB consider training and technology transfer as an integral part of the project. The supplier is required to provide comprehensive and hands on technical training for five (05) SNDB Resources on the complete supplied solution/products and allied equipment by OEM Certified Trainers.

The cost of training should be included in the price schedule of the bidding document. The supplier will provide all necessary installation, technical, troubleshooting, maintenance and preventive maintenance manuals and documentation, CDs, Award of training completion certificates to SNDB staff etc. and keep on updating SNDB for all related technical updates.

The training should be a part of complete solution offering by the supplier that should include but not limited to the following:

1. Complete product introduction, architecture, functionality, technical features, limitations etc.
2. Implementation Installation, configuration, integration, customization, fine tuning, maintenance and services, reporting etc. with respect to the SNDB IT security requirements.
3. Day to day Operation management with available tools, backup and restore procedures in case of product malfunctioning and failure etc.
4. Security operation center monitoring, detection, analytics, reporting, incident handling and ticket escalation etc.
5. Troubleshooting and Maintenance of the System.

3.5 Operational Acceptance

Operational Acceptance means that the supplies and services in the contract have been installed and run in operations after testing in accordance with the products' parameters mentioned in the technical specifications and features meeting the technical requirements of the project.

At least One (01) months of successful operations of the installed system, in accordance with the SNDB required configuration, will confirm the Operational Acceptance of all the supplies under this contract. Also the supplier will ensure dedicated on-site support till operational acceptance.

Any component identified and confirmed through OEM/Distributor or Dealer or by Physical Inspection or performance to be non-genuine, copy or refurbished will be rejected for acceptance and it will be suppliers responsibility to replace that component or system or the entire lot failing which the SNDB may terminate the contract.

For testing any cost associated with test equipment shall be borne by the supplier.

During the course of the project until the operational acceptance of the last installation is signed any cost associated with the repair and/or replacement of the supplies in this contract will remain covered in Warranty and SLA and will be borne by the supplier.

The documentation is a part of operational acceptance that comprised all SNDB specific project related system (hardware, storage, software, Applications) documentation. The supplier will provide following documentation including but not limited to the:

1) System Installations, Configuration and Administration
2) User guides
3) Operation & maintenance (O&M) manual that will cover all components and systems in a way that is easily understood.
4) Troubleshooting, backup and recovery
5) Standard Operating Procedure with snapshots, diagrams, commands etc.

3.6 Technical Requirements

The technical requirements are categorized as under:

1. Architectural and Deployment Requirements
2. Operational Requirements (Administration & Configuration)
3. Logs/Events/Use or Misuse cases Management Requirements
4. Security Intelligence (Real-time monitoring and prevention, Event Correlation, Analysis and Alerting)
5. Network Activity Monitoring
6. Advanced Threat Management
7. Incident Response and Management
8. Information/Logs/Events Source Requirements
9. Reporting
10. Product/Solution Roadmap

3.6.1 Architectural and Deployment Requirements

The following are the architectural and deployment requirements of the system:

Sr. No.	Requirements
1.	The bidder should include the hardware, software/database, The bidder need to supply, install & configure all the required servers, application/software, OS, middleware, back-up software etc for implementation. Hardware storage must be sufficient for 3 years logs. The bid price must include all relevant costs.
2.	The application should have comprehensive predefined security configuration assessment check (settings) for different supported platforms as per industry standards such as ISO27001, PCI-DSS, OWASP, CIS etc
3.	The application should allow search of assets based on IP, Location, Owner and Department
4.	The application should support multiple approaches for vulnerability assessment. 1. Automated Vulnerability Assessment (over the network) 2. Manual Vulnerability Assessment in case automated VA is not allowed
5.	Highly scalable and able to support centralized and distributed environments across multiple sites

6.	Appliance based solution or supplier should propose associated hardware

	and storage to meet and optimized technical requirements as per OEM recommendation.
7.	The solution should support high availability of hardware and storage solution preferably automatic failover for both hardware and software level
8.	Support multiple deployment options (on-premises, all-in-one appliances, virtual appliances, software, virtual image)
9.	Minimum support 1000 EPS/MPS/EPC/MPC or similar with scalability up to 10,000 EPS/MPS/EPC/MPC or similar
10.	Minimum support 10000 network flow/m with scalability up to 100,000 network flow/m
11.	The solution architecture support heavy load from different IT assets for logs collection with no major performance degradation
12.	Support multiple network interface support i.e. dedicated interface for logs/events collection, dedicated interface for network flows, dedicated interface for system administration etc.
13.	Support integration of open source and closed loop applications
14.	Support healthy database for logs, events and network activities collection and processing such that all information can be access from a single GUI in efficient manner.
15.	Ensure the integrity and confidentiality of the information collected from log sources
16.	Robust analytical risk and threat based intelligence engine for event correlation, use cases from multiple collectors and associated log sources
17.	Provision of flexible and ease of integration, retrieval/collection, aggregation, sorting, filtering, searching, correlation and analysis of events, logs or data across all distributed components.
18.	Support Offline Storage and compressed backup for SAN (FC and/or IP)
19.	Support integration with vulnerability and patch management, Identity Access module, Network Admission Control, WLAN Controller, AAA, IPS and Threat intelligence etc. solutions.
20.	Integration with Core Banking of SNDB i.e. ABII System and its alternative system such as ATM Host, Switch, Avanza etc for log collection and rule based alert generation
21.	System should be able to involve remedial process based on rules defined by SNDB
22.	All standard rules as defined by international good practices must be included
23.	Additions of rules should be easy and manageable
24.	Should provide compliance reports as per SBP Guidelines
25.	Should full stack monitoring & management

3.6.2 Moving Forward

License for EPS/MPS/EPC/MPC and Network Flow/m /FPM can be increased as per the requirement

3.6.3 Operational Requirements (Administration & Configuration)

Operational requirements are an integral part of any security intelligence solution.

Sr. No.	Requirements
1	Friendly and Ease of use interfaces (i.e. icons, menu bar, tips & help, drill downs, wizards, command short cuts, favorites etc.)
2	Support both manual and automatic update of configuration information with minimal user intervention. For example, security taxonomy updates, rule updates,
	device support, upgrades, patches etc.
3	Support protected web-based GUI to perform central management of all components, monitored assets, system administration, analysis and reporting tasks.
4	The system ensures all associated system components continue to operate when any other part of the system fails or loses connectivity (i.e., management console goes off-line all separate collectors continue to capture logs).
5	Automated and manual backup/recovery process.
6	Real time dashboard of proposed system internal health checks and performance indicators statistics, i.e. memory, storage, CPU, I/Os, network traffic etc. and notify the system administrator when problems arise.
7	Provide the ability to deliver multiple dashboards that can be customized to meet the specific functional requirements of different users of the system and to achieve and implement the right segregation of duty.
8	The system administrator is able to define role base access to the system by log source, assets group, functional area or dashboard. This includes being able to restrict a user's access to information to only those systems from a specific group or functions or dashboard including, but not limited to, administration, reporting, event filtering, correlation, and/or dashboard viewing.
9	The solution deliver customizable dashboards (i.e. for Security Operation Center, threat management, compliance management, privileged users monitoring, monitored assets view, top security events view, network activities and attacks view, use cases view, malware/virus views, suspicious/malicious activities view, incidents and alarms views etc.).
10	Support and provide predefined templates for dashboards and wizard to build new ones dashboards as per customer requirement or institution IT or business environment.
11	The solution provide intuitive mechanisms for system troubleshooting such as proactive notifications, command line, GUI utilities etc.
12	The solution support versatile and diversified built-in rules for use cases / policies / scenarios implementation
13	The solution supports the selection of built-in and customized dashboards from the UI for use in SOC or NOC deployments.
14	The solution provides the ability to encrypt communications between components. (Data in transit)
15	The solution generate and record audit logs of all administrator / user actions across monitored assets including SIEM system, Core Banking, ADC etc.
16	The solution must not initially drop any events if the license exceeds the purchased license volume and also alert for this situation in advance
17	The solution is able to use the same management console to restore the archived logs to be re-processed, re-normalized and re-classified.

18	The solution maintains a database of all assets discovered on the network. The user should be able to search this database.
19	Support standard protocols (like DNS, NetBIOS, SNMP, NTP, SMTP, HTTPS, SSH).
20	The solution supports manual and/or automated classification and inventory of assets i.e. criticality, location, department, ownership/custodian, H/w & S/w details, etc. that are being monitored and protected.
21	The solution provides integration with Microsoft active directory system
22	The solution supports file integrity monitoring across monitored assets.

3.6.4 Logs/Events/Use or Misuse cases Management Requirements

Sr. No.	Requirements
1	Log collection and archive architecture that supports both short-term (online) and long-term (offline) event storage.
2	The solution support industry log collection methods (Syslog, Windows Management Instrumentation (WMI), Remote Procedure Call (RPC), Windows Events Collection, FTP, SFTP, SNMP, SMTP, JDBC, SDEE etc.)
3	The solution also support non industry log collection methods like Single-line Flat Files, Multi-line Flat Files, Proprietary and customized APIs etc.
4	The solution provide agent-less collection of event logs whenever possible.
5	The solution support long-term access to detailed security event and network flow data for analysis. The system must be able to provide access to at least 12 months' worth of online/active detailed information and additional 12 months offline/passive information and scalable up to 5 years of offline/passive information.
6	The solution / system generate audit logs of all administrator / user actions within system/SIEM Accounting Audit including logs/event tamper monitoring.
7	The solution support custom applications or non-supported devices logs parsing / normalization.
8	The solution supports diversified agent and agent less log collection mechanism.
9	The solution supports and maintains a history of user authentication event on per asset basis.
10	The solution supports built-in use cases as per threat detection, flow analysis, network & application behavioral analysis, incident etc.
11	The solution categorizes log data into a human-readable format to eliminate the need to know OEM specific event IDs.
12	The solution normalizes common event fields (i.e. usernames, IP addresses, hostnames, log source device, commands, time and date stamping etc.) from disparate devices across a multi-OEM network. Specialized parsing/normalization requirements also be supported.
13	The solution provides APIs, GUIs and wizards for parser creation to support the integration of unsupported data sources.
14	The solution provides common taxonomy /categories of events.
15	The solution provides the ability to store/retain both normalized and the original raw format of the event log for forensic purposes.
16	The solution provides the ability to normalize and aggregate event fields.
17	The solution supports normalize event time stamps across multiple time zones.

18	The solution supports the collector/agent send the log over TCP and encrypted from remote locations or secure zone.
19	The solution supports integrity of logs/events collected from all monitored assets

3.6.5 Security Intelligence (Real-time monitoring, Event Correlation, Analytics and Alerting / Alarms)

Sr. No.	Requirements
1	The solution support and provide real-time monitoring of users and networks activities, data access, intrusion, threats and attacks detection, behavioral profiling, suspicious/malicious activities, malware/virus proliferation, affected/compromised hosts, use cases anomalies, monitored assets anomalies, IPs and hostnames reputation, geo locations sessions, advanced persistent threats etc.
2	The solution provides alerting based on observed security events, threats, indicators of compromise from monitored devices.
3	The solution provides alerting based on observed anomalies and behavioral changes in network flow and associated security events and threats. Solution should provide alerts based on rules defined/required by SNDB
4	The solution generates an alert when a system license goes beyond the given threshold in terms of count or percentage and notifies the system administrator.
5	The solution supports alerts on internal health checks and performance indicators statistics beyond given threshold level, i.e. memory, storage, CPU, I/Os, network traffic etc. and notify the system administrator when problems arise.
6	The solution supports an alert mechanism if any SIEM system service / component / monitored asset goes in to non-responsive /stop / hang state and restored back to normal state. The alerts should be customizable as per requirements of SNDB
7	The solution provides the ability to correlate information across potentially disparate devices.
8	The solution supports risk based weighted alerts to allow for prioritization. Weightages must be assignable based on multiple characteristics such as asset type, asset value, threat/attack type, activities type, protocol, application, etc.
9	The solution provides a mechanism, to optimize rule tuning, and customized rule development as per the institution use cases requirements.
10	The solution provides the ability to aggregate an analyze events based on a user specified filter.
11	The solution limits and summarized the presentation of multiple similar events and alerts.
12	The solution supports the ability to correlate against intelligence feed, security data feeds (i.e. geographic mapping, known botnet channels, known hostile networks, etc.). These intelligence feeds should be updated automatically by the solution.
13	The solution supports real time monitor and alert when there is a disruption or disconnection in log collection from an asset or log source.
14	The solution provides a real-time event view of monitored information in raw/original as well as processed/parsed format.
15	The solution provides alerting based upon established policy or rule.
16	The solution supports and provides behavioral white lists and baselines trend from hosts, applications, user activities, networks etc.
17	The solution should be capable of taking automatic actions upon receiving an alert/alarm through email or by ticket/case escalation.

3.6.6 Network Activity Monitoring

Sr. No.	Requirements
1	The solution supports local and remote network traffic collection architecture and analysis.
2	The solution supports up to layer 7 visibility of application definition protocols and ports. The system must support the identification of applications using ports other than the well-known, and applications tunneling themselves on other ports (e.g., HTTP as transport for MS-Instant Messenger should be detected as Instant messenger - not HTTP, TOR, P2P etc.)
3	The solution dynamically learns network behavioral norms and exposes changes as they occur.
4	The solution detects denial-of-service (DoS) and distributed denial-of-service (DDoS) attacks.
5	The solution detects and present views of traffic pertaining to observed threats in the network (e.g. brute force attack, reconnaissance, P2P, command and control communication, SQL injection etc.)
6	The solution identifies inbound/outbound network traffic from potentially risky applications (e.g. file sharing, peer-to-peer, malware etc.)
7	The solution displays traffic profiles in terms of packet rate. This capability must be available for simple TCP analysis (TCP Flags, etc)
8	The solution maintains network profile and present information in multiple timeframes.
9	The solution is able to profile communication originating from or destined to the internet by geographic regions in real-time.
10	The solution provides the ability to extract specific, user defined, fields from network data and use the fields in correlation rules.
11	The solution supports in display visual traffic profiles in terms of bytes, packet rates and number of hosts communicating. These displays must be available for applications, ports, protocols, threats across each configured monitoring point in the network and VLAN.
12	The solution is able to generate useable Metadata for network packets content such as source IP, Destination IP, source and destination Protocols, Database queries, Session Size, Session content including filenames, usernames etc. API should be available for processing the logs by other application as required
13	The solution allows the user to create custom profiles and views using any property of a flow, log, data source or already profiled traffic, IP addresses, groups of IP addresses, source/destination IP pairs etc.

3.6.7 Advanced Threat Management

Sr. No.	Requirements
1	The solution supports and provides threat intelligence feeds include supporting protocols and formats.
2	The solution allows integration with the threat intelligence source/feed and provide real time visibility of global threat landscape automatically as per critical and severity ratings of threat.
3	The solution provides the ability to contextually correlate threat detection on the network and host with security events and real-time knowledge of the assets or network being targeted.
4	The solution provides the ability to automatically weight the priority and severity of reported security threats/events according to the relative importance of the targeted asset.
5	The solution supports IP and domain reputation, geo-location monitoring.
6	The solution supports and provide latest threats information like malware, phishing, suspicious apps, credential theft, breach of security controls, critical and high risk vulnerabilities, command & control reports, suspicious proxies and protocols, exploitation of vulnerabilities, Zero-day malware indicators/vulnerabilities, information leaks, hacktivism etc.
7	The solution supports and have built in Pattern Matching to identify advance yet granular threats e.g. User Account created and privilege escalated, Audit logs cleared and stopped, multiple authentication by single ID from different sources into single destination etc.

3.6.8 Incident Response and Management

Sr. No.	Requirements
1	The solution provides automatic contextual information for incidents and ability to perform basic forensic analysis.
2	The solution supports disparate events belonging to the same incident are automatically aggregated through correlation rules.
3	The solution provides a mechanism to capture all relevant aspects of a security incident in a single logical view. This view should include relevant events, network activity data, correlated alerts, and vulnerability data.
4	The solution allows the fine tuning and reducing of false positives of the Indicator of Compromise, incident, risk scoring, alerts/alarms.
5	The solution supports operational efficiency and efficient workflows through automated and/or manual response capabilities, including automation to improve threat/incident detection and analytics, ticket escalation to the IT operation staff, easy execution, status update, follow up and closure
6	The solution supports triaging of incidents aided by tagging, commenting, annotating, audit trail and real time status tracking of ongoing incidents.
7	The solution provides a mechanism to track security incidents across a wide range of relevant attributes (i.e. IP addresses, usernames, log source, correlation rules, user defined, time date, etc) for forensics purpose. The user must be able to filter incidents along these defined attributes.

3.6.9 Information/Logs/Events Source Requirements

Sr. No.	Requirements
1	The solution supports heterogeneous OEM and open source products like Microsoft, LINUX/UNIX Cisco, CA Technologies, Juniper, McAfee, Temenos, IBM, EMC, FireEye, RSA, APC, Oracle, Symantec, VMWare, HyperVisor, Baracuda, Avaya etc.
2	The solution supports information/logs/events collected from Microsoft based servers (Active Directory/Domain controller, Exchange, Proxy, share point, IIS, SQL, Anti-Virus/Malware, DLP, Gateways, syslogs, sandboxes etc.) and end-user systems.
3	The solution supports information/logs/events collected from Linux/Unix based servers (Apache, syslogs, etc.) and end-user systems.
4	The solution supports information/logs/events collected from enterprise class database solutions (MS SQL, Oracle SQL, JBase etc.)
5	The solution supports information/logs/events collected from proprietary applications (i.e. ERP, T24, SWIFT, Web, RTGS, e-CIB, DWH, OLAP, ABII Core Banking Application, Avanza Rendezvous etc.)
6	The solution supports information/logs/events collected from Data Leak Protection (DLP), File integrity and activity monitoring software and tools.
7	The solution supports information/logs/events collected from Authentication, Authorization and Auditing servers (Access Control Server, Network Admission Control Server, Identity and access management Server, Database Activity Monitoring Server etc.)
8	The solution supports information/logs/events collected from Network infrastructure components (i.e. switches, routers, firewalls, IDS/IPS, sandboxes etc.)
9	The solution supports information/logs/events collected from Network flows (i.e. Netflow, J-Flow, S-Flow etc.) products.
10	The solution supports information/logs/events collected from industry leading vulnerability scanners and patch management solutions.

3.6.10 Reporting

Sr. No.	Requirements
1	The solution provides reporting on high level IT security posture for management in terms of graphics, statistics, past and current trend, Top ratings/severity etc.
2	The solution provides configurable reporting engine for customized report creation.
3	The solution supports on demand and automatic scheduled report generation and distribution in electronic form via e-mail while maintain archiving of reports.
4	The solution provides templates for the easy creation and delivery of reports at multiple levels ranging from operations, business issues to the management,
5	The solution provides reports for typical contextual business and security issues through robust filtering and searching.
6	The solution supports sorting/searching/filtering of reports.
7	The solution supports monitored IT assets scope, ticket escalation and status reports.
8	The solution supports on demand and automated reports of users activities audit, use cases anomalies, networks intrusion and attacks, malware/virus across hosts, affected/compromised hosts, suspicious/illegitimate inbound/outbound network

	activities/traffic, suspicious/malicious sessions, monitored IT assets disconnection, stopped responding, heartbeat failure etc.
9	The solution provides the ability to export the internally generated reports to common file formats. i.e.html, csv, xls, pdf, doc etc. with institution monogram/logo support.
10	The solution provides optional reports for specific compliance regulations (PCI, SOX, FISMA) and control frameworks including (COBIT, ISO).
11	The solution supports real time creation and generation of reports from the dashboard.
12	The solution supports manual and/or automated report on classification and inventory of assets i.e. criticality, location, department, ownership/custodian, H/w & S/w details, installed applications, EOL etc. that are being monitored and protected.
13	The solution supports case/issue/incident management reports i.e. mean time to detect, escalation, pending, deferred, under progress, mean time to resolve/recover etc.
14	The solution supports integrity of generated reports

3.6.11 Product/Solution Roadmap

Sr. No.	Requirements
1	The solution has well established mechanisms to enhance current features, functionality and influence future features and products.
2	The solution has 24x7 well managed online support portal for problems, issues and requirements resolution, ticket escalation, knowledge base, software upgrades/patches.
3	Bidder provides comprehensive warranty, support, and maintenance services of quoted solution during pre and post warranty period.
4	The solution must have minimum 5 years or more end-of-life cycle at the time of bidding
5	At the time of bidding, the proposed solution must be in the leader's quadrant of Gartner.

3.7 Warranty and SLA

3.7.1 Warranty:

01 (one) year onsite comprehensive warranty (with free parts and labor) will commence from the date of Operational Acceptance Certificate.

3.7.2 Service Level Agreement (SLA) during and after Warranty

03 Years SLA	One (01) Year SLA during warranty with one (1) certified and skilled resident engineer and 24x7 OEM backed Maintenance and Support	SLA Will commence from the date of Operational Acceptance Certificate

	Extendable upto Two (02) Years SLA after Warranty with one (1) certified and skilled resident engineer and 24x7 OEM backed Maintenance and Support with mutual consent of both parties	till end of entire contract period.

Any component or equipment identified non-genuine, copy or refurbished during entire SLA will be rejected instantly and it will be supplier's responsibility to replace that component or equipment.

The bidders are required to include OEM warranty with SLA during the warranty period of 1 (one)-year as well as post warranty OEM backed Maintenance and Support of 4 (four) Years with the SLA as mentioned below

The SLA during and after Warranty Maintenance and Support of the supplies should be equipped with the OEM Support Packages to meet the following requirements, except any damage caused by the fire or disaster event or mishandling of the equipment against the specified and communicated standards operating and handling procedures to the SNDB by the OEM/Supplier.

The OEM Support Services will remain available to the SNDB on call 24 x 7 basis.

Telephone, Web and email based case opening for technical problems

Engineers Support (Preferably On-Site) or otherwise over email/phone/web whenever required by the SNDB.

The AHR should be carried out by the supplier for Custom clearing, transportation and on-site delivery of the hardware after Duty Delivery Paid to SNDB meeting the SLA time. The return and collection at customer site and return of faulty items to OEM and its related expenditure is also the responsibility of the supplier.

The warranty of the supplies will start from the Date of Operational Acceptance Certificate of the complete system.

The warranty, Maintenance and Support should be supported and registered by the OEM on the name of SNDB.

3.7.3 Service Level Agreement (SLA) Requirements

3.7.3.1 Scope of Services:

Supplier shall provide support services to run and maintain all the Hardware and Software proposed in the solution in compliance with the Service Level Requirements.

The Supplier shall also replace, restore, reinstall, reconfigure, integrate, customize, troubleshoot, Patch servings and updates, Release (minor and major software/firmware/middleware upgrades), Backup hardware, Support case management (opening, escalation, follow up, historical analysis, reports, knowledge base, etc) through internet based web portal, OEM's Remote technical assistance from acceptable locations to SNDB, Access to technical material, documents, manuals and knowledge base, On- site support as and when required for any failed hardware, storage, software and application components for recovery to normal operational status at no cost to the customer.

3.7.3.2 Availability Requirement:

This section defines the Service Level requirements, classification of incidents, and means of reporting, and expectations for availability and response times in relation to all Hardware, Storage, Software, Application and any add-on or customization performed during implementation (if any) pertaining to their proposed solution that are to be maintained and supported by the Supplier.

Following table outlines the Incident Classification System including required Recovery Time:

3.7.3.3 Reporting Time:

It is the time duration from logging a support incident till the technical support person of the supplier contacts SNDB concerned Technical team.

3.7.3.4 Recovery Time:

It is the time duration from logging a support incident till the problem resolution for restoring faulting system from severity RED to ORANGE or from ORANGE to GREEN. This time starts from problem reported till successful completion of required corrective action, inclusive of replacement (if required).

3.7.3.5 Standard Business Hours:

Normal Business hours: 9:00AM - 5:30PM, Monday through Thursday and 9:00AM – 6:00PM on Friday.

3.7.3.6 Extended Business Hours:

24 x 7

Any change in Standard Business hours by Government of Pakistan will be followed accordingly during entire contract period.

3.8 Reporting & Resolution Time Limits Table

Severity	RED category	Orange category	Green category
Criteria	-Entire production system is down, or a major system component is inoperative or severely impacted - System performance has severely degraded	System is operating normally, but a redundant component or supporting feature has failed. e.g. Log source(s) stopped responding, dashboard not working/freeze, Alerts/Alarms stops, offline storage not available, backup abnormally stopped, License exceeding, Threat intelligence feed(s) not responding or stopped etc. - Technical issues are being faced causing interruptions to the operations or any failure in its functionality due any suspected hardware or software failure	-The system is available and performing adequately, however performance tuning, software or firmware patch installation or software or firmware version upgrade is required during a planned activity. - Operational performance of the appliance / system is facing error(s), while the operations remain functional. -Any query towards the supplied solution raised by the SNDB to the local partner or OEM
Reporting time	Within two **(02) business hours of** Reported Incident	Within six **(06) business hours** of Reported Incident	Within twenty four **(24) business hours** of Reported Incident
Resolution Time	Within six **(06) business** hours of Reporting	Within forty eight **(48) business hours** of Reporting	Within five **(05) business days** of Reporting

Action	- Immediate availability of onsite engineers support for recovery options within one hour - Troubleshoot, Rectify, Repair, Replace faulty component (s), Re-configure, Re-deploy within specified - Escalation to OEM for technical support from OEM via internet or phone - Provide backup solution to continue	- On-Site Technical Support on Call Basis. - Troubleshoot, Rectify, Repair, Replace, Re-install, Re-configure and Re-deploy component (s) to ensure resumption of business operations within specified hours as per requirement - Escalation to OEM for technical support from OEM via internet or phone (if required).	- Technical Support on Call Basis or On-Site as per requirements. - Technical assistance from OEM via internet or phone. - Firmware/software patches updates and upgrades.
	operations until primary or actual solution is restored		
Support Coverage	- 24 x 7	During business days hours (9:00AM - 5:30PM, Monday through Thursday and 9:00AM – 6:00PM on Friday) or otherwise notified by the Government of Pakistan or SNDB on special occasions.	During business days hours (9:00AM - 5:30PM, Monday through Thursday and 9:00AM – 6:00PM on Friday) or otherwise notified by the Government of Pakistan or SNDB on special occasions.

3.9 Terms and Conditions:

3.9.1 The Supplier shall provide details about Help Desk or Customer Support contact information including details about Call Logging Procedure to ensure recording, monitoring and reporting of support calls.

3.9.2 Supplier should provide call logging through telephone in terms of Support Levels and Escalation Procedures that should be mapped to the Severity of the incidents and should also provide telephone number which will be used after Standard Business Hours.

3.9.3 Supplier shall provide details about structure of Technical Support in terms of Support Levels and Escalation Procedures that should be mapped to the Severity of the incidents.

3.9.4 The Supplier shall provide onsite support, maintenance, replacement and update of BIOS, firmware, and all associated software supplied as part of solution covered under this agreement. The Supplier will provide latest version of firmware/software on Customer's request for up gradation purpose free of cost. In case of bug in Software/firmware Supplier will provide required patch and will perform patching, testing and verifying the changes with the coordination of the Supplier (if requested). Upgrade to Latest Version or patch fixing shall be free for the Customer.

3.9.5 Supplier shall submit all incident reports and quarterly summary reports for any support period as and when required.

3.9.6 Supplier shall perform all dispatch functions, including keeping the Customer informed about the status and eventual completion of replacements or repairs.

3.9.7 RED incidents should be given an escalated level of commitment from Supplier. For RED incidents, Supplier shall ask their Support Professionals to work non-standard hours, reassign critical resources from other activities, and/or ensure a Support Professional to work round-the-clock until a problem is fully resolved.

3.9.8 A problem that initially starts at a severity RED situation may be classified at severity ORANGE upon implementing a workaround. When a permanent solution is found and implemented, the problem might be reclassified to severity GREEN for monitoring before it is closed. However, reclassification of severity shall be accepted and signed off by the Customer.

3.9.9 If same fault re-occurs within 48 hours, the original call will be reopened with the same log number and the Recovery Time will continue from the time that original call was re-opened.

3.9.10 In case the faulty item or unit is required to be sent overseas for repair or replacement services then Supplier will send the faulty equipment and deliver the replacement or repaired equipment to the Customer site at its own cost to overseas for repair and replacement.

During and after the warranty period (which means during the entire 5 (five)-years period) the supplier will have to provide support services as per the required SLA mentioned above.

The selected bidder will be essentially required to provide necessary CNIC of the Project Manager, Engineers, Technicians, labors and other logistic resources etc working within the SNDB site during the contract period.

The bidders must adhere to the rules, discipline and practices of SNDB, during the entire course of project.

4 FINANCIAL PROPOSAL

PRICE SCHEDULE

(Applicable for the year 2020-21)

Name of Bidder _____

S #	Description	One Time Cost (in Pak Rupee) (A)	Monthly Recurring Charges (in Pak Rupee) (B)
1	Procurement of SIEM/Log Management System		
	***Total Amount =** One Time Cost (A) + Monthly Recurring Charges(B) x 36 **(In Pak Rupee)**		

Note: The lowest bid will be calculated as per formula above. However initial contract will be given for one year only, which may be extended mutually as per SPPRA Rule.

**This Total Amount will be taken as price 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 Amended 2017.

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

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

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

"GC" mean these General Conditions of Contract.

"Government" means the Government of Sindh.

"Currency" means Pak Rupees.

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

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

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

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

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

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

5.1.2 Law Governing Contract

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

5.1.3 Notice

- Any notice, request or consent required or permitted to be given or made pursuant to this Contract shall be in writing. Any such notice, request or consent shall be deemed to have been given or made when delivered in person to an authorized representative of the Party to whom the communication is addressed, or when sent to such Party at the address specified in the SC.

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

5.1.4 Authorized Representative

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

5.1.5 Taxes and Duties

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

5.1.6 Effectiveness of Contract

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

5.1.7 Expiration of Contract

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

5.1.8 Modifications or Variations

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

5.1.9 Force Majeure

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

5.1.10 No Breach of Contract

The failure of a Party to fulfil any of its obligations under the contract shall not be considered to be

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

5.1.11 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.

5.1.12 Termination

5.1.12.1 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.

5.1.12.2 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

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

g. 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.

5.1.12.3 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:

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

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

5.1.13 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.

5.1.14 Settlement of Disputes

5.1.14.1 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.

5.1.14.2 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.

5.1.15 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.

5.1.16 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.

5.1.17 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.

5.1.18 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.

5.1.19 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.

5.1.19.1 Performance Security

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

5.1.19.2 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.

5.1.19.3 Price

Schedule of prices shall be as fixed in the Contract.

6. BID FORM

Annexure "A"

Dated:_____, 2020

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

Gentelman,

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/Pay order in a sum equivalent to ten percent (10%) of the Contract Price for the due performance of the Contract, in the form prescribed by SNDB.

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

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

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

Name & Address of Agent	**Amount and Currency**
_____	_____

7. BID SECURITY FORM Annexure "B"

Whereas [name of the Bidder] has submitted its bid dated [date of submission of bid] for the *Procurement of SIEM/Log Management System*.

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

THE CONDITIONS of this obligation are:

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

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

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

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

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

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

[Signature and Seal of the Bank]

8. PERFORMANCE SECURITY FORM Annexure "C"

To,

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

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

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

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

This guarantee is valid until the_____day of_____2020.

Signature and Seal of the Guarantors

Name of Bank

Address

Date

9. INTEGRITY PACT Annexure "D"

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: _____

10. SCHEDULE OF OPENING AND SUBMISSION OF BID

Annexure "E"

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

11. FORM OF CONTRACT (Non-Disclosure Agreement)

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 fulfil each Party's confidentiality obligations to the extent the terms set forth below are incorporated therein (the "Purpose").

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

1. The Effective Date of this Agreement is_____2020.

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

   - Trade secrets;
   - Financial information, including pricing;
   - Technical information, including research, development, procedures, algorithms, data, designs, and know-how;
   - Business information, including operations, planning, marketing interests, and products;
   - The terms of any agreement entered into between the Parties and the discussions, negotiations and proposals related thereto; and
   - Information acquired during any facilities tours.

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

   - If it is clearly and conspicuously marked as "confidential" or with a similar designation;
   - If it is identified by the Discloser as confidential and/or proprietary before, during, or promptly after presentation or communication; or
   - If it is disclosed in a manner in which the Discloser reasonably communicated, or the Recipient should reasonably have understood under the circumstances, including without limitation those described in Section 2 above, that the disclosure should be treated as confidential, whether or not the specific designation "confidential" or any similar designation is used.

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

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

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

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

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

   - Make copies of documents containing Confidential Information.

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

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

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

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

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

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

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

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

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

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

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

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

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

Sindh Bank Limited	**Company Name:**
Registered Address:	**Registered Address:**
Name: _____	**Name:** _____
Signature: _____	**Signature:** _____
Title: _____	**Title:** _____
Date: _____	**Date:** _____

12. CONTRACT AGREEMENT Annexure"G"

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	
	I ail	
	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: _____

13. UNDERTAKING/AFFIDAVIT ANNEXURE "I"

To be typed on Rs.50/- Stamp Paper

AFFIDAVIT / DECLARATION

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

I, _____ S/o _____, Proprietor/Authorized Representative/Partner/Director of M/s_____, having NTN #_____, holding CNIC #_____, do hereby state on solemn affirmation as under: -

1. That the above named firm/company has not been adjudged an insolvent from any Court of law.

2. That no execution of decree or order of any Court remains unsatisfied against the firm/company.

3. That the above named firm/company has not been compounded with its creditors.

4. That my/our firm/company has not been convicted of a financial crime.

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

DEPONENT
(PROPRIETOR / REPRESENTATIVE)/DIRECTOR

Solemnly affirmed and stated by the above named deponent, personally, before me, on this_____day of_____2020, who has been identified as per his CNIC. **COMMISSIONER FOR TAKING AFFIDAVIT**