Government of Pakistan

NATIONAL INFORMATION TECHNOLOGY BOARD

(NITB)

Ministry of Information Technology & Telecommunications

Request for Proposal

For Supply of (IT Software & Solution))

Tender No. NITB-4(366)/2023

19th April, 2023

www.nitb.gov.pk

Table of Contents

Data Sheet

Bid Selection Method	One Stage - Two Envelope: The method of selection is: Quality and Cost Based Selection (QCBS). RFP is available under Tender link of NITB website https://nitb.gov.pk and https://www.ppra.org.pk
Bid Security	200,000 PKR
Deliverables	For Supply, Installation, Commissioning, Configuration, Integration & testing **LOT 1 VDI Solution without Thin-Clients** **LOT 2 Software for Vulnerability and PAN Testing** **LOT 3 Software & Licenses (Anti-Virus)**
Contact Person	Deputy Directory (Admin) Email: **ddadmin@nitb.gov.pk** Phone: 051-9265063
Language	Proposals should be submitted in English language
Currency	All prices should be quoted in Pak Rupees
Taxes	The quoted price should include all applicable taxes
Proposal Validity	Proposals must remain valid for 60 days after the submission date
Bidder must submit	Two (02) copies of both technical and financial proposals (One original and one photocopy) A printable and searchable copy in a USB flash drive of technical proposal
Proposal Submission Address	Plot # 24, B, Street No 06, Sector H-9/1, Islamabad
Submission Date & Time	Both Technical proposal & Financial bid must be submitted in two different sealed envelopes on or before **10th May 2023 at 1100 hrs**. Technical proposal shall be opened on the same date at 1130 hrs. **Pre-Bid Meeting on 28th April, 2023 at 1100 hrs.**

Executive Summary

National IT Board (NITB) is an autonomous board and is mandated to undertake and coordinate e-government initiatives at Federal Ministries/Divisions and Departments, provide consulting and advisory services in acquiring and implementing IT solutions as well as IT capacity building of staff of these organizations. NITB intends through this tender to purchase the following items along with installation & configuration services from the eligible bidders. After sale support, warranty and trainings with certification is also required (if applicable).

1. Invitation to Bids

The National Information Technology Board, hereinafter called "NITB" or the 'Purchaser' or the 'Procuring Agency', intends to invite bids against the RFP titled "Supply of (IT Software & Solutions) from eligible Bidders.

1.1 PPRA Rules to be followed

Public Procurement Regulatory Authority (PPRA) Rules (Public Procurement Rules, 2004) will be strictly followed. These may be obtained from PPRA's website.

In this document, unless otherwise mentioned to the contrary, "Rule" means a Rule under the Public Procurement Regulatory Authority Rules, 2004.

1.2 Mode of Advertisement(s)

As per Rule 12, this RFP is being placed online at PPRA's and NITB websites, as well as being advertised in print media.
Bidding document containing detailed instructions, terms and conditions and this advertisement can be downloaded from NITB and PPRA websites.

1.3 Type of Open Competitive Bidding

As per PPRA rule 36 (b), One-Stage - Two Envelope Procedure shall be followed.

- The bid shall comprise a single package containing two separate envelopes. Each envelope shall contain separately the financial proposal and the technical proposal.
- The envelopes shall be marked as "FINANCIAL PROPOSAL" and "TECHNICAL PROPOSAL" in bold and legible letters to avoid confusion.
- Initially, only the envelope marked "TECHNICAL PROPOSAL" shall be opened.
- The envelope marked as "FINANCIAL PROPOSAL" shall be retained in the custody of the procuring agency without being opened.
- Technical Proposal shall contain separate envelop of 200,000/- PKR which will be opened along with Technical Proposal.
- The Bidders will be first checked for the eligibility, as per the requirements in eligibility criteria. Thereafter, all eligible bidders shall be shortlisted against the technical requirements.
- The shortlisted Bidders will be technically evaluated and those securing a minimum of 60 marks in the technical evaluation (LOT Wise) will be qualified for Financial Evaluation.

- In case of only one bidder (LOT Wise) secures equals to or greater than 60 marks in technical evaluation, NITB may decide to lower the cut-off score for technical qualification but not less than 50 marks
- After the evaluation and approval of the technical proposals, the procuring agency shall open the financial proposals of the technically accepted bids, publicly at the time, date and venue announced and communicated to the bidders in advance, within the bid validity period.
- The financial proposal of bids found technically non-responsive shall be returned un-opened to the respective bidders.
- The contract may be awarded to bidder(s) securing highest combined score of Technical plus Financials Bids. The overall bid score has been divided as follows:
- Technical Proposal Evaluation carries 70% weightage.
- Financials Proposal Evaluation carries 30% weightage.
- The procuring agency may reject all bids or proposals at any time prior to the acceptance of a bid or proposal. The procuring agency shall upon request communicate to any Bidder who submitted a bid or proposal, the grounds for its rejection of all bids or proposals, but is not required to justify those grounds.
- The procuring agency shall incur no liability, solely by virtue of its invoking sub-rule (1) towards Bidder who have submitted bids or proposals.
- Notice of the rejection of all bids or proposals shall be given promptly to all Bidders that submitted the proposals.

2. Instructions to Bidders

2.1 Language

The Bid and all documents relating to the Bid, exchanged between the Bidder and the Purchaser, shall be in English. Any printed literature furnished by the Bidder in another language shall be accompanied by an English translation which shall govern for purposes of interpretation of the Bid.

2.2 Bid Document

The bid document can be downloaded from the NITB or PPRA websites.

2.3 RFP Clarifications and Questions

To ensure fair consideration for all Bidders, NITB prohibits communication to or with any department, officer or employee during the evaluation process.

No bidder shall be allowed to alter or modify his bid after the bids have been opened. However, the procuring agency may seek and accept clarifications to the bid that do not change the substance of the bid.

Any request for clarification in the bid, made by the procuring agency shall invariably be in writing. The response to such request shall also be in writing.

2.4 Pre-Bid Meeting

A pre-bid meeting may be scheduled according to '**Annexure A**' at the NITB premises to respond to queries of interested bidders.

Queries from the Bidders (if any) for seeking clarifications regarding the specifications of the services must be received in writing to the NITB. Only written queries will be responded in the pre-bid meeting. NITB reserve the right not to address any verbal query during meeting (pre-bid meeting), Phone calls or any other verbal medium.

Bidders should note that during the period from the advertisement of the Bid till the receipt of the bid, all queries should be communicated to a dedicated contact person(s), mentioned in this document, in writing via e-mail or post only. Please include the following reference as the subject of your email/letter: "Supply of (IT Equipment, Hardware, Software and Miscellaneous items".

Response to any Participant's inquiries will be made in writing by NITB in a timely manner to all prospective Participants. Any oral interpretations or clarifications of this RFP shall not be relied upon.

Bidders are also required to state, in their proposals, the name, title, fax number and e-mail address of the bidder's authorized representative through whom all communications shall be directed until the process has been completed or terminated.

Any changes or clarification resulting from the pre-bid meeting will be shared in writing by NITB. NITB will not be responsible for any costs or expenses incurred by bidders in connection with the preparation or delivery of bids.

2.5 RFP / Bid Price

The quoted price shall be:

- In Pak Rupees
- Inclusive of all taxes, duties, levies, insurance, freight, etc.
- Best / final / fixed and valid until completion of all obligations under the Contract i.e., not subject to variation / escalation.
- Including all charges up to the delivery point / closeout.
- If not specifically mentioned in the Bid, it shall be presumed that the quoted price is as per the requirements given in this document, where no prices are entered against any item, the price of that item shall be deemed to be free of charge, and no separate payment shall be made for that item(s).
- Withholding Tax, Sales Tax and Other Taxes: The Bidder is hereby informed that the NITB will deduct tax at the rate prescribed under the Tax Laws of Federal Government of Pakistan, from all payments for products and services rendered by any Bidder who signs a contract with NITB.

2.6 RFP Schedule

Critical dates and milestones in connection with this RFP.

2.6.1 Timeline of the project:

Delivery Time will be 45 to 60 Days after the issuing of PO.

2.6.2 Ownership of the project:

All the Equipment and related software in the project shall be the property of Government of Pakistan with packages and licenses.

2.6.3 Technology Transfer

The vendor will be bound to deliver complete technology and to provide running development environment. The Vendor shall be bound to provide three (03) years warranty for LOT# 1, 2 & 3 of the installed equipment and onsite support & Maintenance services for one (03) year after the Final Acceptance Certificate.
For Lot# 1, OEM presence is required during the deployment of solution.

3. Confidentiality

The Bidder (whether or not he submits a Proposal to the RFP) shall treat this RFP document and its details as confidential. No information pertaining to this RFP or the examination, clarification, evaluation, comparison and award of this RFP shall be disclosed to other Bidders or any other persons not officially connected with the RFP process, including, but not limited to, the Bidder's own affiliate companies and subsidiaries. The Bidder is not permitted to make any public announcement or release any information regarding this RFP without NITB's prior written approval.

NITB reserves the right to share the Bidder's response to this RFP with its advisors and affiliates. In the event the Bidder commits a breach of confidentiality, NITB reserves the right to disqualify the Bidder from this RFP process and furthermore not include the Bidder in any future similar exercises.
NITB is not responsible for declaration of the short-listed Bidder(s).
The Bidder shall state clearly those elements of its response that it considers confidential and/or proprietary. Failure to properly identify and mark confidential or proprietary information may result in all information received being deemed non-confidential, non-proprietary, and in the public domain.

3.1 Notices

In this document, unless otherwise specified, wherever provision is made for exchanging notice, certificate, order, consent, approval or instructions amongst the Parties, the same shall be:

In writing

- Issued within 05 working days.
- Served by sending the same by courier or registered post to their principal office as they shall notify for the purpose and.
- The words "notify", "certify", "order", "consent", "approve", "instruct", shall be construed accordingly.
-

3.2 Option to Bid

The bidders can Bid for any number(s) LOTs.

3.3 Joint Venture

No Joint Venture is allowed

3.4 Corrupt Practices

NITB requires that bidders / 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.
NITB will reject a proposal for award, if it determines that the bidder recommended for award was engaged in any corrupt or has been blacklisted.
Any false information or misstatement on the part of the bidder will lead to disqualification/ blacklisting/ legal proceeding regardless of the price or quality of the product.

3.5 Penalty

a) If the bidder fails to complete the Assignment within the given timeline as defined in the ToRs and agreement, Penalty of 0.1% of the total contract value (total bid amount) per week (Five working days will be considered as one week) will be charged up to maximum of 20% of the agreement/contract value. Thereafter, work order will be cancelled, the agreement will be terminated and in addition to penalty the Performance Guarantee will be forfeited.

b) In case of non-satisfactory support and maintenance services by the bidder during the contract term and as determined by the NITB, the Penalty at rate of 0.1% per day of the contract value will be applicable on the lead bidder until the performance is improved up to the satisfaction of NITB.

3.6 Warranty /Support & Maintenance Services

The Contractor shall provide comprehensive three (03) years warranty along with onsite support and maintenance for LOT# 1, 2 & 3. During this period, it will be the responsibility of the Contractor to rectify any defects and provide services such as preventive maintenance, configuration of equipment, problem rectification within the permissible downtime and backup equipment inventory. The necessary patches, upgrades and updates as and when released by the OEM shall also be provided during the warranty period so as to ensure that the system is functioning to provide the best performance.
For Lot# 1, it is required to perform Preventive Maintenance in every six months with the three (03) years of warranty.

4. Indemnification

By Bidder: Bidder will, at its own expense, indemnify and hold harmless NITB, and their respective officers, directors, employees, representatives, licensees and agents from and against and in respect of any and all claims, liabilities, allegations, suits, actions, investigations, judgments, deficiencies, settlements, inquiries, demands or other proceedings of whatever nature or kind, whether formal or informal, brought against NITB or any of their respective officers, directors, employees, representatives, licensees or agents, by any third parties against and in respect of any and all damages, liabilities, losses, costs, charges, fees and expenses, including without limitation reasonable legal fees and expenses, as and when incurred, relating to, based upon, incident to,

arising from, or in connection with any claim or allegation with regard to any misrepresentation by the bidder, breach of any provision of this document by the bidder, negligence or willful misconduct of the contractor, infringing in any manner any copyright, trademark, intellectual property, trade secret or patent of any third party. The foregoing obligation is subject to NITB giving bidder a prompt written notice of any claim and giving the bidder sole control of the defense of such claim. Bidder agrees that it may not, without NITB's prior written consent, as the case may be, enter into any settlement or compromise of any claim that results in any admission of liability or wrongdoing on the part of NITB, as the case may be.

To the fullest extent permitted by law, the bidder shall indemnify and hold harmless NITB and their respective officers, directors, employees, representatives, licensees and agents from and against claims, damages, losses and expenses, including but not limited to legal fees, arising out of or resulting from performance of the work under this document in relation to any claim, damage, loss or expense attributable to bodily injury, sickness, disease or death to the bidder's personnel or any third party hired by the bidder or to injury to or destruction of tangible property.

5. Preparation of Bid

5.1 Cost of Bidding

The issuance of this RFP and the receipt of information in response to this RFP shall not in any way cause NITB to incur any liability or obligation to the bidder (and /or any proposed Subcontractor(s), if any), financial or otherwise. NITB assumes no obligation to reimburse or in any way compensate the bidder for costs and/or expenses incurred in connection with the bidder's Proposal in response to this RFP. All costs and expenses incurred by the bidder (and/or any proposed subcontractor(s), if any) pertaining to all activities in the preparation, submission, review, selection and negotiation of the bidder's proposal in response to this RFP shall be borne by the bidder (and/or any proposed subcontractor(s), if any) ("costs and expenses").

5.2 Bid Security / Earnest Money Deposit (EMD)

In accordance with PPRA Rules 2004, Rule 25, the Bidder will submit a bid security of 200,000/- PKR of the total quoted price in shape of Bank Draft/Bank Guarantee in favor of National Information Technology Board.

- The Bid Security issued by any scheduled bank of Pakistan will be acceptable. Cheques will not be acceptable in any case. Bid security of the successful bidder will be returned once the Performance Guarantee is submitted to NITB.
- The bid security shall be part of technical bid envelope, failing to do so will cause rejection of the bid.
- Bid security envelope will be opened at the time of submission and opening of technical proposal
- The Bid Security shall be forfeited by the Purchaser on the occurrence of any/all of the following conditions:
- If the Bidder withdraws the Bid during the period of the Bid validity specified by the Purchaser or
- If the Bidder, having been notified of the acceptance of the Bid by the Purchaser during the period of the Bid validity, fails or refuses to furnish the Performance Security, in accordance with the Bid Document.

- The Bid security shall be returned to the technically unsuccessful Bidder with unopened/sealed financial bid.
- While the unsuccessful bidders of technical bid opening procedure will be returned the Bid Security only within one-month period.
- Validity of the Bid Security should be 60 days minimum.

5.3 Technical Proposal

Bidders are required to submit the technical proposal stating a brief description of the bidder's organization outlining their recent experience along with Data Sheet(s) of the product(s) bidder has offered

Names of professional staff details profile has to be submitted.

Refer Annexure B – Submittal Requirements for Technical Proposal.

5.4 Financial Proposal

The Financial proposal shall be prepared using the standard form attached, duly signed by the authorized representative of the bidder.
The bidder shall provide its list of costs with all items described in the technical proposal priced separately. Refer Annexure C – Submittal Requirements for Financial Proposal.
In case a bidder is participating in multiple Lots than pricing shall be provided LOT Wise.

5.5 Payment Terms / Schedule

Payments will be made by NITB against the invoice/s raised by the bidder by following the procedure in vogue against each milestone on production of following documents:
Sales tax invoice duly signed and stamped by the organization.
NITB shall issue the Provisional Acceptance Certificate (PAC) after delivery, delivery challan shall be signed by Admin Department of NITB. Vendor shall be responsible to get the delivery challan sign-off.
There will be no Advance payment / mobilization.
Following is the payment schedule based on defined milestones:

Sr No.	Milestones	Payment %	Remarks
1	Provisional Acceptance Certificate (PAC)* a) Supply of the equipment c) Signing off of delivery Challan	70%	For particular PO
2	Staff Training **	20 %	
3	Final Acceptance Certificate (FAC) ***	10%	
4	Release of performance guarantee ****	After compilation of Warranty Period	

**Provisional Acceptance Certificate (PAC) includes the sign-off from the nominated person(s) from NITB, for following:*

- *Installation & commissioning*
- *Configuration & Integration*
- *Testing of infrastructure and related software*
- *License Bundles.*

*** Technical Training includes:*

- *Trainings through Certified professionals*

**** Final Acceptance Certificate (FAC) includes:*

- *Work Completion Certificate*

***** Release of performance guarantee:*

- *After the completion of three-years support & Maintenance for installed infrastructure*

5.6 Bid Currencies

Bids are to be quoted in USD. Conversion Rate will be applied on the Date of Financial Opening

5.7 Advice of Omission or Misstatement

In the event it is evident to a bidder responding to this RFP that NITB has omitted or misstated a material requirement to this RFP and/or the services required by this RFP, the responding bidder shall advise the contact identified in the RFP Clarifications and Questions section above of such omission or misstatement.

5.8 Bid Validity Period

The bid shall have a minimum validity period of Sixty (60) days from the last date for submission of the Bid. The Procuring Agency may solicit the Bidders consent to an extension of the validity period of the bid. The request and the response thereto shall be made in writing. Bid Security shall also be suitably extended.

5.9 Additional Charges

No additional charges, other than those listed in the financial proposal, shall be made. Prices quoted will include verification/coordination of order, all costs for shipping, delivery to the site, setup, installation, training etc.

5.10 Right to Request Additional Information

NITB reserves the right to request any additional information that might be deemed necessary during the evaluation process.

5.11 Right of Refusal

The procuring agency may reject all bids or proposals at any time prior to the acceptance of a bid or proposal. The procuring agency shall upon request communicate to any Bidder who submitted

a bid or proposal, the grounds for its rejection of all bids or proposals but is not required to justify those grounds.
The procuring agency shall incur no liability, solely by virtue of its invoking sub-rule (1) towards Bidder who have submitted bids or proposals.
Notice of the rejection of all bids or proposals shall be given promptly to all Bidders that submitted the proposals.

6. Submission of Bids

6.1 Sealing and Marking of Bids

Bid shall comprise a single sealed package containing two separate sealed envelopes. Each envelope shall contain separately the financial proposal and the technical proposal. Envelope shall be marked as "FINANCIAL PROPOSAL" and "TECHNICAL PROPOSAL" in bold and legible letters to avoid confusion.
The bids along with the bid security, must be dropped at: National Information Technology Board.
Technical Proposal must contain Sealed BID Security envelop which would be opened at time of opening of technical proposal.
All submissions are due to the attention of the authorized person, no later than the date and time specified in Annexure A. Any proposal received after the due date and time will not be accepted by NITB.
Proposal submissions must be organized according to the instructions provided in this and separately packaged, sealed and identified as follows:

- Identify as Technical or Financial Proposal
- Title: Supply of (IT Equipment, Hardware, Software and Miscellaneous items)
- NITB, Plot No 24B, H-9, Islamabad, Pakistan.
- Proposal submissions must include the following copies:
- One (1) original version of the entire Technical Proposal with original signatures.
- One (1) envelope containing BID Security must be submitted along with technical proposal
- One (1) photocopied version of the entire Technical Proposal.
- One (1) softcopy containing the entire Technical Proposal.
- One (1) original version of the Financial Proposal with original signatures.
- One (1) photocopied version of the entire Financial Proposal.
- One (1) softcopy containing the entire Financial Proposal.

Softcopies of Technical as well as financial proposal are required to be submitted in the form of USB in the respective sealed envelopes. The files must be unprotected, editable, electronic documents and must be clear of any viruses, imbedded documents, or executable links.

6.2 Extension of Time Period for Submission of Bids

NITB may extend the deadline for submission of bids, if the following condition exists.

- If Procurement Committee is convinced that such extraordinary circumstances have arisen owing to law-and-order situation or a natural calamity that the deadline should be extended.
- If Purchase Committee decides to extend the deadline due to any administrative reason.

6.3 Late Bids

Late bids shall not be considered. Therefore, it is suggested that the response be sent in a manner that ensures it arrives on time, for example: through verifiable courier, Registered Mail or in person. Responses through Fax, email, and non-registered delivery through Pakistan Post Mail will not be considered.

6.4 Presentation by Bidders

Bidders may be asked to present their proposal as per the terms and conditions listed along with the announcement of this RFP. The Bidder will be required to provide and present a detailed and comprehensive project management plan that will become the sole source for determining implementation tasks and completion time of each task. The bidders are expected to present the technical proposal and the various components within the overall proposal. The bidder must be able to answer all queries and question of the evaluation/procurement committee within the presentation.

6.5 Modification or Withdrawal of Proposals

Proposal modification and withdrawal terms and conditions are governed PPRA rules and Regulations. Such laws and regulations shall always prevail at all times. Under no circumstances shall a bidder be allowed to modify or withdraw his proposal if such actions are prohibited by the relevant Bid laws.

6.6 Submittal Requirements

- For Technical Proposal, please ensure that the listed requirements in "Annexure B" are provided.
- For Financial Proposal, please ensure that the listed requirements in "Annexure C" are provided.

7. Opening and Evaluation of Bids

7.1 Opening of Bids by NITB

Initially the envelopes marked "TECHNICAL PROPOSAL" and "BID Security" shall be opened and envelope marked as "FINANCIAL PROPOSAL" shall be retained in the custody of the NITB without being opened. NITB shall evaluate the technical proposal without reference to the price and may reject any proposal which does not comply with the specified requirements.

7.2 Modification of Bids

No bidder shall be allowed to alter or modify its bids after the expiry of deadline for the receipt of the bids unless, NITB may, at its discretion, ask a bidder for a clarification of bid for evaluation purposes. The request for clarification and the response shall be in writing and no change in the prices or substance of bid shall be sought, offered or permitted.

7.3 Missing Information

Information requested in this document is aimed to evaluate the bidder and their system in a best possible way, therefore NITB encourage bidder to furnish the information as requested in this document. Any missing information shall be considered as not available.

7.4 Addendum or Supplement to Request for Proposal

At any time prior to the deadline for submission of the Bid, NITB may, for any reason, whether on its own initiative or in response to a clarification request by prospective bidder, modify the RFP by issuing addenda.

A summary of all questions and responses as well as any adjustments regarding the scope of this Bid - if any, will be prepared and distributed to all potential bidders that submitted their intent to bid. (if any, changes will be reflected in the revised proposal published at NITB and PPRA Websites)

7.5 Shortlisting of the Bidders

Shortlisting will purely be based on the information provided in the submitted proposal and related documents, where the eligible bidder would acquire at least 60 score in the given technical evaluation criteria.

7.6 Current References

The Bidder must provide in the proposal the names and complete contact information of at least three (3) client references in prescribed format under Annexure-D who:

Are able to discuss Bidder's performance in providing solutions similar to those contemplated in this RFP, and have agreed to be contacted by NITB representatives. NITB expects the bidder to contact their client references to confirm their availability to speak with NITB during this time.

7.7 Bidder Evaluation

Contract(s) shall be awarded at the sole discretion of NITB after evaluation of the bidder's proposal, reference discussions, negotiations, determination of competitive advantage and cost. Bidder must have a satisfactory record of contract performance, integrity, business ethics, adequate financial resources (in the opinion of NITB) and vision to meet the contractual requirements contemplated in this RFP. By submitting a proposal, the Bidder warrants that:

a) It is legally authorized to provide the subject solution(s) globally or locally,
b) It is in compliance with all applicable laws and regulations,
c) It is not prohibited from doing business with NITB/GoP by law, order, regulation or otherwise, and
d) The person submitting the proposal on behalf of the Bidder is authorized to bind it to the terms of the proposal.

An evaluation committee ("Technical Evaluation Committee") specifically formed for this RFP process will evaluate all submitted proposals. Proposals may be evaluated and eliminated without further discussions and at the sole discretion of NITB. NITB will be the sole initiator of discussions to clarify or negotiate the proposal offerings. The NITB evaluation committee will evaluate each proposal based upon their understanding of the proposals. The NITB evaluation committee will conduct a fair, impartial and comprehensive evaluation of all proposals. If applicable, a contract

shall be awarded, taking into consideration the best interests of NITB. The selection criteria is defined in subsequent section and may include:

a) Experience of the bidder with similar projects, size and scope
b) Management and staff profiles
c) Solution differentiation and implementation approach
d) Details of Scalability, Performance, Integration, Configurability, Parameterization
e) Cost/Value/Favorable contract terms & conditions

NITB reserves the right to award a contract without any further discussion with the bidder(s) who have submitted proposals in response to this RFP. Therefore, proposals should be submitted initially on the most favorable terms available to NITB from a price, contractual terms and conditions, and technical standpoint. However, NITB reserves the right to conduct discussions with Bidders who submit proposals that pass the initial screening process for the feasibility of the solution(s).

NITB is not under any obligation to reveal, to a bidder, how a proposal was assessed or to provide information relative to the decision-making process.

NITB shall evaluate a bidder's "confidence in its own ability to perform" based on a bidder's willingness to provide NITB with meaningful contractual assurances and remedies NITB may exercise in the event of that Bidder's non-performance.

7.8 Proposal Acceptance

A proposal submitted in response to this RFP shall constitute a binding offer. Acknowledgment of this condition shall be indicated by the signature of the Participant bidder or an officer of the Participant bidder legally authorized to execute contractual obligations. A submission in response to this RFP acknowledges acceptance by the Participant of all terms and conditions including compensation, as set forth herein. A Participant shall identify clearly and thoroughly any variations between its proposal and the NITB's RFP. Bidder shall ensure that every page of their proposal is signed and stamped.

7.9 Availability of Professional Staff / Experts

Having selected the bidder on the basis of, among other things, an evaluation of proposed professional staff, the NITB expects to get the contract executed by the professional staff named in the proposal. Before contract negotiations, the NITB shall require assurances that the professional staff shall be actually available. NITB shall not consider substitutions during contract negotiations unless both parties agree that undue delay in the selection process makes such substitution unavoidable or for reasons such as death or medical incapacity. If this is not the case and if it is established that professional staff were offered in the proposal without confirming their availability, the Bidder may be disqualified. Any proposed substitute shall have equivalent or better qualifications and experience than the original candidate and his name be submitted by the Bidder within the period of time specified in the letter of invitation to negotiate.

7.10 Alternative Provisions

Alternative proposals are not allowed.

7.11 Redressal of Grievances by the Procuring Agency

The Purchaser will constitute a committee comprising of odd number of persons, with proper powers and authorizations, to address the complaints of bidders that may occur prior to the entry into force of the procurement contract.

- Any bidder feeling aggrieved by any act of the procuring agency after the submission of his bid may lodge a written complaint concerning his grievances within seven days of announcement of the technical evaluation report and five days after issuance of final evaluation report.
- The GRC (Grievance redressal committee) shall investigate and decide upon the complaint within ten days of its receipt
- In case, the complaint is filed after the issuance of the final evaluation report, the complainant cannot raise any objection on technical evaluation of the report
- Any bidder or party not satisfied with the decision of the GRC, may file an appeal before the Authority within thirty days of communication of the decision subject to depositing the prescribed fee and in accordance with the procedure issued by the Authority. The decision of the Authority shall be considered as final.

8. Award of Contract

8.1 Award Criteria

NITB shall award the contract to the successful bidder, whose bid has been determined to be substantially responsive in the view of our requirements & expectations and has provided the most competitive bid, provided further that the bidder is determined to be qualified to perform the contract satisfactorily.

8.2 NITB's Right to Accept Any Bid and to Reject Any or All Bids

NITB reserves the right to accept or reject any Bid, and to annul the bidding process and reject all bids at any time prior to contract award, without thereby incurring any liability to the bidder(s).

8.3 Notification of Award

Prior to the expiration of the period of bid validity, NITB 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, NITB will promptly notify each unsuccessful bidder.

8.4 Signing of Contract

Within Fifteen (15) days from the date of notification of the contract award, the successful bidder shall furnish to NITB particulars of the person who would sign the contract on behalf of the successful bidder along with an original power of attorney executed in favor of such person. Draft contract will be shared with the successful bidder only.

8.5 Performance Security

Within (15) days of the receipt of notification of award of Contract from the Procuring Agency, the successful Bidder will furnish the Performance Security and sign the Contract. The value of Performance Security shall be 10% of the bid value to be issued by any scheduled bank of Pakistan having "A" rating. The Performance Security will remain valid till FAC sign off.

8.6 RFP Response Ownership

All information, materials and ideas submitted become the property of NITB upon submission. NITB reserves the right to modify, reject or use without limitation any or all of the ideas from submitted information. All information, materials and ideas contained in the Bidder's proposal can be used by NITB without any restriction, provided that NITB will not disclose any financial and pricing information the Bidder designates as confidential with any other potential Bidder. NITB reserves the right to share, disclose or discuss to any of its consultants any proposal in response to this RFP in order to secure expert opinion. Please submit the softcopies of technical and financial proposals in USB / CD / DVD, along with the respective proposal in sealed envelopes.

8.7 Integrity Pact

The successful bidder(s) shall upon the award of the contract execute an Integrity Pact with NITB. [Specimen is attached in Annexure-G]

8.8 Non-Disclosure Agreement

The successful bidder(s) shall upon the award of the contract execute a Non-Disclosure Agreement with NITB. [Specimen is attached in "Annexure H"]

8.9 Contract Terms and Conditions

The successful bidder(s) shall upon the award of the contract, agree and sign a formal contract with NITB, which shall be based on the terms and conditions in this document, PPRA contractual guidelines and NITB's contractual requirements.
Wherever in conflict with the RFP and the contract or no safeguard of NITB is mentioned, the stipulation of PPRA 2004 as internally adopted by NITB shall prevail.

8.10 Mandatory support and Maintenance period

The vendor shall be bound to provide mandatory onsite support and maintenance after the PAC Signing-Off without any additional cost for three (3) Year.

9. Scope of Work

9.1 Lot 1 VDI Solution (Without Thin- Client):

01	Complete VDI Solution	50

9.2 Lot 2 Software for Vulnerability and PAN Testing:

01	Software for Vulnerability and PAN Testing	01

9.3 Lot 3 Software & Licenses (Anti-Virus):

01	Anti-Virus End-to-End Solution (100 with 3-years subscription)	100

10. Integration of Existing Hardware.

Successful bidder will be required for integration of existing System and network.

11. Trainings

The bidder will be responsible for the Free of cost (FOC) trainings and certifications (voucher where applicable) of the employees in the areas of implementation, operations, management, error handling, network and system administration of in-scope solutions.

12. Evaluation Process

12.1 Eligibility

Below is the criterion for the eligibility of the interested Bidders. These are all mandatory requirements and failing to comply will result in ineligibility for further technical evaluation. Please ensure complete and valid documentary evidences are provided, NITB reserves the right to check the authenticity of any submitted document.

S.No	Criteria	Compliance (Yes/No)
1.	Bidder is a registered/incorporated company in Pakistan with SECP at least for the last 02 years for all Lots	
2.	Bidder has a valid Registration Certificate for Income Tax, Sales Tax and/or other allied agencies / organizations / regulatory authorities	
3.	Bidder is an Active Taxpayers as per Federal Board of Revenue (FBR)'s database i.e. Active Taxpayer List (ATL)	
4.	Bidder Affidavit on Judicial / Stamp Paper attested by Notary Public which certifies to provide three-years warranty/guarantee after installation.	
5.	Affidavit on Judicial / Stamp Paper duly attested by Notary Public that the bidder is not blacklisted by any government / semi government Department.	
6.	MAL Certificate from the OEM	

Note: Verifiable documentary proof is required for all above mandatory requirements.

12.2 Technical Evaluation Criteria and Bidder's Response

Bidder(s) are required to provide their responses on the following sheet:
Note:

<table>
<tr><th>SR. NO</th><th>EVALUATION CRITERIA</th><th>MAX MARKS</th></tr>
<tr><td>1.</td><td><u>Financial Capability (for Lot# 1 & 3):</u>
The bidder in had minimum an average annual turnover of PKR 100 million of past (02) financial years between 1st July, 2020 and 30th June, 2022.
Calculation Criteria:
100 million to 150 million -10 marks
151 million to 200 million -20 marks
201 million or above -30 marks

<u>Financial Capability (for Lot# 2):</u>
The bidder in had minimum an average annual turnover of PKR 100 million of past (02) financial years between 1st July, 2020 and 30th June, 2022.
Calculation Criteria:
50 million to 75 million -10 marks
76 million to 100 million -20 marks
101 million or above -30 marks</td><td>30</td></tr>
<tr><td>2.</td><td><u>General Work Experience (for All Lot):</u>
Bidder MUST provide evidence in the form of completion certificate of projects within last 2 years.
Calculation Criteria:
One (01) – 10 marks
Two (02) – 20 marks
Three (03) –25 marks</td><td>25</td></tr>
<tr><td>3.</td><td>Team Capacity
Dedicated resources with minimum 2 years relevant experience to work on the tasks. Companies to provide resource profiles/CVs (Annexure-F) along with proof of their employment with the company.
Calculation Categories:
<table>
<tr><th>Resource Type</th><th>No.</th><th>Marks</th><th>No.</th><th>Marks</th><th>No.</th><th>Marks</th></tr>
<tr><td>Product Specialist (Certified)</td><td>1</td><td>3</td><td>2</td><td>6</td><td>3+</td><td>8</td></tr>
<tr><td>Installation Specialist</td><td>1-2</td><td>3</td><td>3-4</td><td>6</td><td>4+</td><td>8</td></tr>
<tr><td>Product Support Specialist</td><td>1-2</td><td>4</td><td>3-4</td><td>8</td><td>4+</td><td>9</td></tr>
</table></td><td>25</td></tr>
<tr><td>4.</td><td>Presentation on Solution</td><td>20</td></tr>
<tr><td colspan="2">TOTAL MARKS</td><td>100</td></tr>
</table>

NOTE:	
i.	**Total Technical Marks = 100 Marks**
ii.	**Minimum Technical Qualifying Marks = 70 Marks**
iii.	**Financial Marks 100 Marks**
iv.	**Weightage of Technical Marks is 70%**
v.	**Weightage of Financial Marks is 30%**

12.3 Technical Proposals Evaluation Summary

- The Bidders shall be first checked for the eligibility, as per the requirements in eligibility criteria. Thereafter, all eligible bidders shall be shortlisted against the technical requirements.
- The shortlisted Bidders shall be technically evaluated and those securing a minimum of 60 marks in the technical evaluation will be qualified for Financial Evaluation.
- In case of only one bidder secures equal to or greater than 60 score in technical evaluation, NITB may decide to lower the cut-off score for healthy competition but not less than 50 marks in technical qualification.
- After the evaluation and approval of the technical proposals, the procuring agency shall open the financial proposals of the technically accepted bids, publicly at the time, date and venue announced and communicated to the bidders in advance, within the bid validity period.
- The financial proposal of bids found technically non-responsive shall be returned un-opened to the respective bidders.
- The contract may be awarded to bidder(s) securing highest combined score of technical plus Financials Bids. The overall bid score has been divided as follows:
    - Technical Proposal Evaluation carries 70% weightage whereas
    - Financials Proposal Evaluation carries 30% weightage.

Please see below the formula for calculating the weightage:

a) Technical score calculation: Bidder's Score= (Points Obtained in Technical Domain/Total points of Technical Domain) x 100
b) Financial score calculation: Bidder's Score= (Min Bid Value / Bid in Consideration) x 100
c) Total score = (Technical Score x 70%) + (Financial Score x 30%)

13. Technical Specification of Equipment/Services

13.1 Lot# 1 VDI Solution (Without Thin Client):

S. No.	Description
1.	**Hardware Specifications**
1.1.	Slot Chassis:12 x 3.5" Disk Slot Chassis
1.2.	Cores: 2 x Gold 6248R(24cores 3.0GHZ Clock Speed)
1.3.	DIMM Slots: Minimum 24 DIMM Slots
1.4.	RAM: 20 x 32GB RDIMM
1.5.	Storage for OS: 2 x 128G SSD (RAID 1)
1.6.	Storage for Cache: 2 x 1.92TB SSD Mixed Use)
1.7.	Storage for Data: 6 x 4TB 7.2K RPM SATA
1.8.	Network Interfaces: 2 x 10Gbps (Optical Ports with SFPs) and 6 x 1Gbps Base-T
1.9.	Other Ports: 2 x USB2.0, 2 x USB3.0, 1 x VGA
1.10.	Power Supply Must Have Redundant
1.11.	Warranty: 3 Years Onsite Support Hardware Warranty
2.	**Software Specifications**
2.1.	**General Requirement**
2.1.1.	VDI Solution with Hyper-Converged Infrastructure Architecture
2.1.2.	HCI, VDI Software and Servers should be from same vendor
2.1.3.	OEM presence in Pakistan for minimum 3 years
2.1.4.	Minimum 5 VDI deployment locally (with in Pakistan)
2.1.5.	50 Concurrent VDI Licenses required
2.1.6.	Warranty & Technical Support: 3 years with Software upgrade & 24x7 Technical Support
2.1.7.	During onsite configuration & installation, OEM resources should present
2.1.8.	Onsite Training: OEM participant(s) required during Training
2.2.	**Virtualization Management Software**
2.2.1.	Must support Role-Based Management with Permission Control
2.2.2.	Must support HTML5 Web Management
2.2.3.	Must support Centralized Control & Visibility
2.2.4.	Must support future scale out Up to 10-12 Nodes
2.3.	**Compute Virtualization Hypervisor**
2.3.1.	VM Snapshot, VM Clone, VM vMotion is required
2.3.2.	Distributed Resource Scheduler (DRS) is required
2.3.3.	Distributed Switch by using Cluster-Level Network Aggregation is required
2.3.4.	Hardware health check to monitor CPU, Memory, Network Interface Card, Hard Drive and RAID Controller is required
2.4.	**Storage Virtualization**
2.4.1.	Must Be the Same Vendor as Compute Hypervisor
2.4.2.	Must support 2 copies & 3 copies data redundancy
2.4.3.	Must support Data Striping Technology
2.4.4.	Must support SSD Cache & SSD Data Tiering
2.4.5.	Must support Data Disk Balancing & Data Rebuilding

2.5.	**Virtual Desktop & Application Virtualization**
2.5.1.	Licensed Soft Client required
2.5.2.	Supported OS: Linux Virtual Desktop, Windows Virtual Desktop
2.5.3.	Provision Multiple Virtual Desktops to Single User
2.5.4.	Template Update with Unified Applications or Updates Installed
2.5.5.	Integration with Microsoft AD for Active Directory Login Authentication
2.5.6.	Role-Based Policy for Different Virtual Desktop and User Binding
2.5.7.	Centralize Power-On All Virtual Desktops According to Time Schedule
2.5.8.	Centralize Power-Off All Virtual Desktops According to Time Schedule
2.5.9.	Integrated Shutdown (Linked Shutdown)
2.5.10.	Virtual Network Independence for Virtual Desktop Access i.e. The intranet anomaly of VMs does not affect access and use of the virtual desktop
2.5.11.	Linked Clone Technology for Dedicated Desktops mode
2.5.12.	Software Distribution and Template update for the Dedicated Desktops mode
2.5.13.	Authentication via soft-client
2.5.14.	Multi-Endpoint Security Restriction Mode, not just IP Address based
2.5.15.	Info Collection of connected soft-client with Details such as Online Status, IP Address, Last Login User, Last Login Time and etc.
2.5.16.	Must Support Software Client Installer to Connect Virtual Desktop from Windows OS, iOS, Android and etc.
2.5.17.	Data Leak Protection on USB Storage such as “Read Only” & “Disabled”
2.5.18.	File Exporting Audit with Report Center (Log all files information transferred to external USB storage)
2.5.19.	Full Screen transparent Watermark with Username
2.5.20.	Virtual Desktop Data Drive Encryption
2.5.21.	Protection against Brute-Force attack with Word Captcha
2.5.22.	Application Virtualisation for Applications such as Internet Explorer, Microsoft Office, Google Chrome and etc.
2.5.23.	Micro-segmentation for east west traffic isolation between VMs.
2.6.	**Virtual Desktop Backup Software Solution**
2.6.1.	Fully Compatible with Compute Hypervisor
2.6.2.	Full VM Level Backup
2.6.3.	Backup VMs in All Hardware Nodes
2.6.4.	Incremental Backup Technology & Difference Backup Technology
2.6.5.	Automated Schedule Backup (Weekly, Daily, Hourly)
2.6.6.	Backup Repository to Internal Virtual Storage
2.6.7.	Backup Repository to External SAN Storage
2.6.8.	iSCSI, FC, Network File Sharing Protocol

13.2 Lot# 2 Software for Vulnerability and PAN Testing:

S. No.	Description
1.	**Requirements for the solution structure and functions**
1.1.	The system must include the following functional components:
1.1.1.	Access control subsystem
1.1.2.	Analysis configuration subsystem

1.1.3.	Security analysis subsystem
1.1.4.	Result visualization and reporting subsystem
1.1.5.	Statistics subsystem
1.1.6.	Data storage subsystem
1.1.7.	Integration subsystem
1.2.	The access control subsystem must provide for granting the System users permissions to access the System functions.
1.3.	The analysis configuration subsystem must provide for configuring scan settings used by the modules in the security analysis subsystem.
1.4.	The security analysis subsystem must provide for testing an application for vulnerabilities and signs of undocumented features.
1.5.	The result visualization and reporting subsystem must provide for displaying results of conducted research and generating reports.
1.6.	The statistics subsystem must provide statistics based on application scan results.
1.7.	The data storage subsystem must provide centralized storage of the results of existing research and the System settings with multi-user remote access.
1.8.	The integration subsystem must provide for the System integration with the Customer's related information systems.
2.	**General System requirements**
2.1.	The system must provide for testing source code of applications written in PHP, Java, C#, Visual Basic .NET, Python, Objective C, Swift, C/C++, Go, JavaScript, Kotlin, and SQL (the PL/SQL, T-SQL, and MySQL dialects).
2.2.	The system must provide classification IDs of detected vulnerabilities according to the categories defined in the following documents and classifiers:
2.2.1.	OWASP Top 10 2017
2.2.2.	OWASP Mobile Top 10 2016
2.2.3.	PCI DSS 3.2
2.2.4.	SANS Top 25
2.2.5.	NIST 800-53 (revision 4)
2.2.6.	Common Vulnerabilities and Exposures (CVE)
2.2.7.	Common Weakness Enumeration (CWE)
3.	**Access control subsystem requirements**
3.1.	The access control subsystem must provide for:
3.1.1.	User authentication for accessing the System functions using the Microsoft Active Directory service.
3.1.2.	Access control of the System functions including:
3.1.2.1.	Listing Microsoft Active Directory (MS AD) users that have the System global administrator permissions.
3.1.2.2.	Listing Microsoft Active Directory (MS AD) users that have the System project administrator permissions.
3.1.2.3.	Listing Microsoft Active Directory (MS AD) users that have permissions to access the System operation results.
4.	**Analysis configuration subsystem requirements**
4.1.	The configuration subsystem must provide for:

4.2.	Selecting a programming language of an analyzed application or its module.
4.3.	Entering the address of an application website used for automated vulnerability confirmation and dynamic analysis.
4.4.	Selecting individual modules in the security analysis subsystem used for application analysis.
4.5.	Selecting operation modes for the source code analysis module.
4.6.	Editing the user signature base of the source code module that contains descriptions of potentially harmful functions, trusted data filtering functions, and user vulnerability types.
4.7.	Selecting operation modes for the third-party vulnerability analysis module.
4.8.	Editing the custom rule base of the third-party vulnerability analysis module.
4.9.	Configuring the dynamic analysis module:
4.9.1.	Scope of performed checks
4.9.2.	Additional HTTP /HTTPS headers passed to the application during checks through the dynamic analysis module
4.9.3.	Proxy server settings
4.9.4.	Authentication mode in the application used during checks:
4.9.5.	No authentication
4.9.6.	Basic HTTP/HTTPS authentication
4.9.7.	Form-based authentication
4.9.8.	Cookie-based authentication
4.10.	Configuring authentication settings sent to the application during testing.
4.11.	Editing rules for automated security assessment of the analyzed application (security policy).
4.12.	Configuring email notifications sent when analysis is completed.
4.13.	Selecting file types to be ignored during application analysis.
5.	**Security analysis subsystem requirements**
5.1.	The security analysis subsystem must include the following modules:
5.1.1.	Source code analysis module
5.1.2.	Automated vulnerability confirmation module
5.1.3.	Dynamic analysis module
5.1.4.	Vulnerability analysis module for third-party libraries
5.1.5.	Configuration file analysis module
5.2.	The source code analysis module must provide for:
5.2.1.	Scanning web application source code for vulnerabilities using the static application security testing method (SAST).
5.2.2.	Scanning web application source code for vulnerabilities using the interactive application security testing method (IAST).
5.2.3.	Finding exploitable vulnerabilities with automatic generation of a vulnerability exploitation script.
5.2.4.	Finding second-order vulnerabilities that can be exploited by an attacker after performing preliminary actions in the application and/or its environment.
5.2.5.	Finding potential vulnerabilities that can be exploited by an attacker if the application code is further developed.

5.3.	The automated vulnerability confirmation module must:
5.3.1.	Provide for a full check to confirm a vulnerability.
5.3.2.	Automatically set the vulnerability confirmation status to "Autoconfirmed" when the subsystem is in the full check mode.
5.4.	The dynamic analysis module must provide for vulnerability detection in applications using the dynamic application security testing (DAST) method.
5.5.	The vulnerability analysis module for third-party libraries must:
5.5.1.	Identify names and versions of third-party libraries used by the application.
5.5.2.	Detect vulnerabilities in third-party libraries used in the application by matching a library name and version against the vulnerability knowledge base data.
5.5.3.	Support custom signatures for identifying and detecting vulnerabilities in third-party libraries.
5.5.4.	Provide vulnerability data including:
5.5.4.1.	Vulnerable component name and version
5.5.4.2.	Path to a file that contains a vulnerable component
5.5.4.3.	Vulnerability description, recommendations, and links to additional information
5.6.	The configuration file analysis module must:
5.6.1.	Provide for analysis of web server and application server configuration files for correct configuration of settings that affect application security.
5.6.2.	Provide vulnerability data including:
5.6.2.1.	Parameter or setting name
5.6.2.2.	Parameter or setting value
5.6.2.3.	Parameter or setting recommended value
5.6.2.4.	Path to a vulnerable file
5.6.2.5.	Vulnerability description, recommendations, and links to additional information
5.7.	Provide for shortening the time spent on each consecutive source code security check using the incremental analysis.
5.8.	Provide for starting an analysis from the command line interface (CLI) to support further integration with the Customer's third-party components.
5.9.	Provide for automated assessment of source code compliance with the security policy based on the results of application source code analysis and verdict delivery.
5.10.	Support deployment to additional hosts (scan agents) to gradually improve the subsystem performance.
6.	**Requirements for the result visualization and reporting subsystem**
6.1.	Provide vulnerability data including:
6.1.1.	Number and contents of a code line considered as the best place to fix a vulnerability
6.1.2.	Number and contents of a code line containing a vulnerability
6.1.3.	Signature of a vulnerable function
6.1.4.	Path to a vulnerable file
6.1.5.	Contents of the vulnerability exploit script
6.1.6.	Additional conditions that must be met to exploit the vulnerability

6.1.7.	Vulnerability description, recommendations, and links to additional information
6.2.	Provide detailed data on an application operation when exploiting a vulnerability.
6.3.	Provide for management of analysis results including:
6.3.1.	Viewing vulnerabilities that match the selected source code directory in the application
6.3.2.	Grouping detected vulnerabilities by:
6.3.2.1.	Type
6.3.2.2.	Best place to fix
6.3.3.	Filtering detected vulnerabilities by:
6.3.3.1.	Severity level
6.3.3.2.	Type
6.3.3.3.	Additional conditions
6.3.3.4.	Confirmation status
6.3.4.	Searching for detected vulnerabilities in the list
6.4.	Provide for separate vulnerability checks by running a vulnerability exploitation script generated by the security analysis subsystem.
6.5.	Provide for editing a vulnerability exploitation script generated by the security analysis subsystem.
6.6.	Provide for viewing the results of executing a vulnerability exploitation script, including the application server's response message and time.
6.7.	Provide for keeping a previously set vulnerability confirmation status after a repeated application analysis if a corresponding vulnerability still exists in code.
6.8.	Provide for setting one of the following vulnerability confirmation statuses manually:
6.8.1.	Confirmed
6.8.2.	Discarded
6.8.3.	No status
6.9.	Provide for creating tasks in an issue tracking system based on Jira.
6.10.	Provide for generating reports based on application analysis results containing detected vulnerabilities with the following information:
6.10.1.	Number and contents of a code line containing a vulnerability
6.10.2.	Signature of a vulnerable function
6.10.3.	Path to a vulnerable file
6.10.4.	Additional conditions that must be met to exploit a vulnerability
6.11.	Provide for including data that describes application operation details when it exploits a corresponding vulnerability as well as a code fragment considered as the best place to fix a vulnerability.
6.12.	Allow uploading user report templates to the System.
6.13.	Support filter-based report generation.
6.14.	Support generation of PDF and HTML reports.
7.	**Statistics subsystem requirements**
7.1.	Web interface for accessing statistics based on application scan results.
7.2.	Statistics on the number of vulnerabilities of various severity levels.

7.3.	Information on changes in the number of vulnerabilities of various severity levels.
7.4.	Statistics with the ability to filter information by project, scan date, and vulnerability severity.
7.5.	Project search by name.
7.6.	Navigation to the result visualization and reporting subsystem to obtain detailed information on scan results.
8.	**Data storage subsystem requirements**
8.1.	Storage of application analysis results, scan settings, and user permissions.
8.2.	Remote access to application analysis results through the visualization subsystem.
8.3.	An application programming interface (API) for remote access to application analysis results.
9.	**Integration subsystem requirements**
9.1.	Information exchange implementation between the System components and the Customer's related information systems.
9.2.	Integration with the following related information systems:
9.2.1.	Version control systems based on Git, TFS, Subversion, Mercurial, GitHub, Bitbucket, Rational ClearCase
9.2.2.	Continuous integration systems based on Jenkins, TeamCity, TFS, GitLab
9.2.3.	Issue tracking systems based on Jira
9.3.	Transferring to related continuous integration systems a verdict based on the results of an application security policy compliance assessment to make an automatic decision whether or not to continue building the application.
10.	**Requirements for information exchange between system components**
10.1.	Components included in the System must use TCP and UDP as standard network protocols for information exchange.
11.	**Technical support requirements**
11.1.	As part of the warranty service, during the license validity period, the System manufacturer or the Contest participant must provide free consultation services (technical support) in English within one business days. Including:
11.1.1.	Troubleshooting errors in the System software
11.1.2.	Providing updates to the System software
11.1.3.	Consulting on the System software operation by phone or email

13.3 Lot# 3 Software & Licenses (Anti-Virus):

	Specifications	
01	**Management Solution**	
	Management Solution	Enables centralized policy management and enforcement for your endpoints and enterprise security products
		Flexible security management
		Organize managed systems in groups to monitor, assign policies, and schedule tasks
		Allow users access to specific groups of systems or give administrators full control
		Unify security management across endpoints, networks, data, and compliance solutions from its own and third-party solutions
		Define how the management solution software directs alerts and security responses based on the type and criticality of security events in your environment.
		Architecture supports hundreds of thousands of devices on a single server, and complex and diverse environments
		supports reporting across on-premises and cloud security information.
		A single web interface aligns security processes for maximum visibility, while a single agent reduces the risk of endpoint conflicts.
		Drag-and-drop dashboards provide security intelligence across endpoints, data, mobile, and networks.
		Shorten response time through actionable dashboards with advanced queries and reports.
		identifies unknown assets on your network, and brings them under control.
	Architecture	Must support 3 tier architecture for UI, data storage and application
	Application Server	Manages and deploys security products, upgrades, and patches.
		Connects to the solutions update server to download the latest security content
		Enforces policies on your endpoints
		Collects events, product properties, and system properties from the managed endpoints and sends them back to management solution
		Reports on the security of your endpoint
	Database	Stores all data about your network-managed systems

	Agent	Agent installed on clients provides:
		Communication to the server for policy enforcement, , and connections to send events, product, and system properties to the management solution for all DLP endpoint and network components
		product deployment and software updates for the DLP components
		Secures Agent-server communications
		Provides communications that occur at regular intervals between your endpoints and the server
	Web console	Allows administrators to log on to the management console to perform security management tasks, such as running queries to report on security status or working with managed software security policies.
	Distributed repositories	Hosts your security content locally throughout your network so that agents can receive updates more quickly.
	Agent Handlers	Reduces the workload of the server by off-loading event processing and agent connectivity duties.
		Agent Handler in DMZ - Supports specific port connections to Agent Handlers installed in the DMZ allowing you to connect through a firewall.
		Management server connects to your LDAP server for RBAC and user based policies
		Automatic Responses- Notifies administrators and task automation when an event occurs. What are the available tasks for Automatic responses ?
	Endpoint Protection	
	Capability	The solution must support common Microsoft Windows desktop operating systems
		The solution must support common Microsoft Windows server operating systems
		The solution must support common Microsoft Windows embedded operating systems
		The solution must support common Linux operating systems
		The solution must support common MacOS operating systems
		The solution must fully support installation & operation on endpoints running in the Public Cloud (e.g. AWS - Amazon Web Services and Microsoft Azure environments).
		The solution must fully support installation & operation on endpoints running on Virtual Environments

	System & Policy Management	This section highlights how Endpoint Security can be managed, and how the default policy configuration can be customized to meet organizational requirements
	Capability	A single management solution to install, manage, configure end point security solutions such as Anti-malware, Reputation platform, real-time communication brokers, Unified Data Loss Prevention technology, Disk Encryptio, File and Removable, media encryption
		The solution must provide central management from an enterprise console
		The solution must allow different roles to manage different products
		The solution must allow to create and manage report
		The solution must have a possibility to audit the changes
		The solution must provide one management console and one agent only
		The solution must support distribution of different product Versions on different system Structures
		The solution must support assignment of different Policies to different system structures
		The solution must have default reports and allow user to create own reports
		The solution must have following default Reports:
		· Systems based on management hierarchy
		· Product Version on the Systems
		· Signature version on the Systems
		· Events
		· Action based on event
		The solution must allow to create and send Reports via Mail based on scheduled time
		The solution must allow the assignment of the policies direct to Endpoint, to management hierarchy, groupings etc.
		The solution must allow to import and export the policies
		The solution must allow to set the inheritance of the Policies and provide the possibility to break the inheritance on specific point
		All of the event data must be saved in the Database
		The solution must support Database on virtual Server
		Which possibility deliver the solution to query the database
		The solution must scale to an estate of at least 250,000 endpoints

		The solution must support multiple Active Directory domains from a single management instance
		The solution must provide API access
		Malware detection
		This section highlights the Malware Detection Methods of the Endpoint Security Solution
		Detection methods
		The system must allow for behavior-based detection of anomalous behavior on the endpoint
		The solution must take an action (whitelist, block) based on a hash value.
		The solution must provide an enterprise reputation based on hash value.
		The solution must provide protection against zero Days, Unknown binaries.
		The solution must provide machine learning statically and dynamically,
		The solution must provide a containment for patient Zero, and thwarting mechanizes
		The solution must provide Ransomware protection,
		The solution must provide memory exploit prevention
		The solution must provide Comprehensive solution architecture that is able to consistently detect and block both unknown and known malware that exploit end-user systems via the web or opening data-at-rest files on enterprise file stores
		The solution must provide Ability to detect client-side EXPLOITS or complex malware embedded within multiple versions of each of the following application file types (this is a representative/partial list): pdf, doc, docx, xls, xlsx, ppt, pptx, flv, f4v, mp3, mp4, tiff, rtf, zip, Java, and JAR
		The solution must Identify and stop both inbound malware and outbound malware communications to Command & Control servers. The solution must Scan data-at-rest within enterprise file shares to detect and quarantine objects containing malware that are waiting for an end-user to open the malicious content.
		The solution must Detect sophisticated hidden threats. The range of detection techniques will be also affected by the type of data gathered. Three realms of data are most valuable: user, endpoint and network events. This data should also be put into context with global threat intelligence (that is, attribution and trends).

		Vendor must explain detection methods employed (known bad, algorithms, decoy, etc.)
		The solution must Utilize Virtual Machine technology, in real- time, at the edge of the enterprise network, to positively identify malware, including zero-hour vulnerability exploits, polymorphic payloads, and obfuscated objects such as java- script, flash content, images, media files, and executables.
		The solution must Identify malware delivered and communicating across multiple network protocols, including WEB (http, https), and File Transfer (ftp).
		The solution must Utilize a Global Malware Intelligence Network to benefit from information gathered by the research efforts of the vendor in a unidirectional fashion.
		The solution must Generate real-time Malware Notification Alerts via the GUI as well as via SNMP, HTTP, and SMTP.
		The solution must Identify Malware with greater than 99% accuracy.
		The solution must be a Signature less detection
		Identify and block previously UNKNOWN malware
		The solution must Immediately distribute malware indicators of compromise and call-back blocking information between all system appliances with the enterprise network; thus preventing an identical attack from being successful in multiple locations The solution must have global research centers to detect incidents in different countries
		The solution must Immediately distribute inbound malware blocking rules and outbound malware call-back blocking rules to other enterprise systems that are able to enforce such blocking rules.
		The solution must check the local reputation cache for the file
		If the file is not in the local reputation cache, the solution must query the reputation server, if available, for the reputation
		If the file is not in the reputation server database, the server queries Global intelligence for the reputation.
		Depending on the file's reputation and allows these settings:
		The file is allowed to run.
		The file is cleaned.
		The file is blocked.
		The file is allowed to run in a container.
		The user is prompted for the action to take.

		For a process with a Known Trusted reputation, solution rules determine the appropriate actions for the process.
		The Reputation server updates the database and sends the updated reputation information to all ATP-enabled systems to immediately protect your environment.
		The Solution must monitor the process, its children, and ancestors for suspicious behaviour, which can indicate a file less attack, and blocks the process if needed
		If the process reputation is Unknown or lower, enhanced remediation backs up changes, and rolls back if the process exhibits malicious behaviour
	Capability	The solution must provide Endpoint Security modules
		The solution must handle Client-side Caching interactions
		The Solution must provide possibility to control the Log/debug Level remotely on Client
		The Solution must provide possibility to run scheduled On Demand Scans
		The Solution must provide possibility to run local On Demand Scans
		The solutions must have an endpoint Firewall
		The solutions must have an endpoint web protection
		The solutions must have an endpoint threat prevention
		The solution must stays up to date, explain
		The solution must use AMCore content
		The solution must provide threat intelligence decision-making,
		The solution must provide protection to OS critical areas like windows register, DLL, APIs, System
		The solution must be able to quarantine files without deleting them if the files are found to possibly be malicious
	Performance	The solution update file size must be at the minimum
		The solution must provide the Ability to run the scan only when the CPU idle
		The solution must provide the Ability to run the scan only when the computer is locked
		The solution must provide the Ability to schedule scan in different times
		Integration
		This section shows how the solution can integrate with other solutions to enhance overall capabilities and deliver additional outcomes.

	Capability	The solution must integrate with other protection technologies, to provide additional capabilities
		The solution must allow integration into a connected architecture to allow instant information sharing between endpoints, systems, and devices in the environment
		The solution must integrate with a network-based sandbox solution.
		The solution must integrate with on premise reputation service.
		The solution must integrate with a cloud-based reputation service.
		The solution must support out of the box protocol to share threats messaging without using APIs.
	Alerting and Responding	This section shows how the solution can generate alerts and allow responses to these alerts to be achieved.
		*Capability
		The solution must provide multiple alerting methods.
		The solution must provide multiple monitoring methods.
		The solution must support the triggering of automated actions in response to an alert.
		The solution must support the use of SHA2
		The solution must publish the reputation over data exchange layer Protocol
		The solution must alert if attempts are made to tamper with local configuration
	Reporting	This section shows how the solution can provide flexible reporting both within the management system, and to external systems.
	Capability	The solution must provide consolidated and prioritized alerts
		The solution must provide powerful reporting capabilities within the management tool.
		The solution must provide customizable reporting capabilities
		The solution must allow reports be generated and delivered automatically
		The solution must report information to a SIEM
		The solution must allow reactions be instigated from the SIEM to trigger endpoint protection
		The solution must provide an inventory of all applications present across the environment
		The solution must provide logging around events and search/query options within logs to undertake investigations

		The solution must provide real-time audit or activity logs for all processes, users, and administrator activity
		The solution must be able to provide logging data for Splunk
		The solution must provide a file name, checksum, count, and order the count (most common and least common) of applications found across the organization
		The solution must provide a Syslog alert feed or native SIEM integration for alerts
		The solution must provide an accurate timestamps of alerts in UTC and local time
	App Control	
	Capability*	The solution must block unauthorized executables on servers, corporate desktops, and fixed-function device
		The solution must uses dynamic whitelisting to guarantee that only trusted applications run on servers, devices, and desktops so it eliminates the need for IT administrators to manually maintain lists of approved applications
		The solution must allow IT control over endpoints to help enforce software license compliance
		The solution must use a dynamic trust model and innovative security features to prevent advanced persistent threats (APT) without requiring signature updates. It guarantees protection without impacting productivity
		The solution must Prevent any malicious, untrusted, or unwanted software from being executed.
		The solution must Automatically identify trusted software and grant it authorization to run.
		The solution must Block users from introducing software that poses a risk to the company.
		The solution must be able to be deployed in a centrally managed environment or in an unmanaged environment, also called standalone, or self-managed.
		The solution must alllow easy search for useful information such as:
		Applications added this week
		Uncertified binaries
		Systems running outdated versions
		Files with unknown reputations in a managed environment
		The solution must extend coverage to executable files,

		libraries, drivers, Java applications, ActiveX controls, and scripts for greater control over application components
		The solution must enforce control on connected or disconnected servers, virtual machines, endpoints, and fixed devices, such as kiosks and point-of-sale (POS) terminals
		The solution must lock down protected endpoints against threats and unwanted changes, with no file system scanning or other periodic activity that might impact system performance
		The solution must offer multiple memory-protection techniques to prevent zero-day attacks
		The solution must prevent whitelisted applications from being exploited by memory buffer overflow attacks on Windows 32- bit and 64-bit systems
		The solution must allow you to switch to Observe mode to discover policies for dynamic desktop environments without enforcing a whitelist lockdown. This mode helps to deploy the software in pre-production environments without affecting the operation of existing applications.
		The solution must integrate with a reputation source to receive reputation information for files and certificates.
		The solution must, Based on the reputation received from one of these sources, allow or ban the execution and software installation
		The solution must integrate with management solution for consolidated and centralized management, and a global view of enterprise security from a single console that manages endpoint protection, data protection as well
		In an unmanaged environment the solution must create whitelist of all authorized executable files. When you run an executable file that isn't whitelisted, the software blocks its execution.
		The solution must protect all files in the whitelist and can't be changed or deleted
		An executable binary or script that isn't in the whitelist is said to be *unauthorized* and is prevented from running.
		The solution must store the whitelist for each drive or volume locally in unmanaged environment
		The solution must support a list of these types of files to be included in the whitelist.
		Binary executables (.exe, .sys, and .dll files)
		Script files (such as .bat, .cmd, and .vbs files)

		When you execute a file on a system with a whitelist, the solution must compare the checksum and path of the binary with the checksum and path stored in the whitelist and allows the execution only if the checksum value and path match.
		The solution must operate in four different modes
		In Disabled mode, the solution must be installed and is not running on the system and features are disabled
		The solution in disabled mode must be able to switch to Observe, Update, or Enabled mode
		Enabled mode must allow only whitelisted applications and files are allowed to run. Execution of unauthorized software, such as a virus or spyware, is prevented
		In enabled mode, solution protects files in the whitelist from unauthorized change
		When in enabled in a managed environment, the solution must support reputation-based execution
		When you execute a file, the solution must fetch its reputation and that of all certificates associated with the file to determine whether to allow or ban the file execution
		The solution must work with Reputation server and Global Intelligence to fetch reputation information for a file
		In Observe mode, the solution is running but it only monitors and logs observations
		In Observation mode, the solution does not prevent any execution or changes made to the endpoints. Instead, it monitors execution activities and compares them with the local inventory and predefined rules
		In Observation mode, solution supports reputation-based execution. When you execute a file, Application Control fetches its reputation and that of all certificates associated with the file to determine whether to allow or ban the file execution.
		All files that are allowed to run in Observe mode are automatically added to the whitelist, if not already present in the whitelist. An observation is logged that corresponds to the action the solution takes in Enabled mode.
		Update mode indicates that protection is effective but changes are allowed on protected endpoints. . In Update mode, all changes are tracked and added to the whitelist.

		When you perform software updates in Update mode, Application Control tracks and records each change. Also, it dynamically updates the whitelist to make sure that the changed or added binaries and files are authorized to run when the system returns to Enabled mode
		If you delete any software and program files from the system, their names are also removed from the whitelist.
		In a managed environment, Update mode supports reputation- based execution. When you execute a file at an endpoint, the software fetches the file's reputation and the reputation of all associated certificates to determine whether to allow or ban the file execution
		The solution must allow Switching between modes From Observe mode, you can switch to Enabled or Disabled mode. From Enabled mode, you can switch to Disabled, Update, or Observe mode. From Update mode, you can switch to Enabled or Disabled mode. From Disabled mode, you can switch to Enabled, Update, or Observe mode.
	DLP	
	Features	Must Identify North America compliance data (HIPAA, GLBA, SOX)
		The Solution must Identify credit card information
		The Solution must Identify personally identifiable information (ID numbers, driver's license, passport)
		The Solution must Identify North America bank account and routing numbers
		The Solution must Identify acceptable use violations like offensive language and images
		The Solution must Identify sensitive corporate operations documents (Governance, Procedures)
		The Solution must Identify sensitive corporate business documents (Legal, M&A, Marketing)
		The Solution must Identify sensitive design documents (CAD, Source Code, Drawings, Project Plans)
		The Solution must Identify European compliance data
		The Solution must Identify Asia Pacific compliance data
		The Solution must Identify other foreign national compliance data

		The Solution must Identify international bank account and routing numbers (SWIFT, IBAN, ABA)
	Policies, Incident Workflow, and Incident Management	Solution must have a Pre-built policies to identify all compliance and information criteria listed above
		Solution must have a New rules That can be created by creating a copy of an existing rule
		Solution must have a Rules that can be tested and tuned using historical information stored on the DLP system
		Solution must have a Rules that can be created based on LDAP attributes including department, geographic location, and group membership
		Exceptions must be built into the rules to minimize false positives
		All DLP incidents from the components must report to a central management console:
		Data-in-motion + Data-at-Rest
		All DLP policies from all components must be managed from a central management console:
		All DLP Components
		Policy violation must retains source IP address, destination IP address, protocol, and port
		Policy violation must retains sender e-mail address, recipient e- mail address, and SMTP headers
		Policy violation retains all content in the transaction, not just the content that violated policy
		Policy violation must retains all attachments in the transaction, not just the attachment that violated policy
		Incidents must assigned automatically to reviewers
		Incidents must sorted by severity level
		Incidents must be sorted by sender, recipient, source, destination, protocol, and content type
		Incidents must display and highlight a summary content that violated the policy
		Incident views must customized based on content pertinent to the reviewer's role and preferences
		Incident reporting must shared with SYSLOG compatible systems
		Multiple incidents must assigned to a case for further investigation and remediation
		Cases must re-assigned to different stakeholders after creation

		Case content must exported with full content and attachments for review by an external reviewer
		Data retention and searching
		Data-in-motion
		Must Indexes and retains all unfiltered network traffic that the network sensor analyses
		Must Indexes and retains all documents sent over unfiltered network traffic
		Must Conduct searches of any e-mail sent from or to email addresses
		Must Conduct searches of any traffic sent from or to IP addresses or URLs
		Must Conducts searches of any traffic sent across protocols or ports
		Must Conduct searches for documents leaving the network based on document type
		Must Conduct searches for any content leaving the network based on keywords
		Must Conduct searches for any content leaving the network based on expressions
		Must Conduct searches for any document leaving the network based on MD5 hash
		Must Conduct searches for any content leaving the network during a specified time period
		Data at rest
		Must Indexes and retains all unfiltered files that are analyzed while scanning file servers
		Must Indexes and retains all unfiltered files that are analyzed while scanning desktops/laptops
		Must Indexes and retains all unfiltered files that are analyzed while scanning SharePoint
		Must Conduct searches for content indexed during a data-at- rest crawl based on keywords
		Must Conduct searches for content indexed during a data-at- rest crawl based on document type
		Must Conduct searches for content indexed during a data-at- rest crawl based on file owner, path, or age
		Must Conduct searches for any document indexed during a data-at-rest crawl based on MD5 hash
	Roles, access, and security	Must Restrict access to specific policy violations based on company role (Compliance, HR, Legal, Finance, etc.)
		Must Restrict access to policy violations on a per group basis
		Must Restrict access to policy violations on a per user basis

		Must Restrict access to actionable functions within polices based on role (Reviewer, Policy Writer, Investigator)
		Must Limit access to incident details and attachments based on role
		Must Mask PII or PCI information contained in match summary display based on role
		Must Restrict access to after-the-fact search capabilities based on role
		Must Restrict access to case creation, reviewing, modification, or deletion based on role
		Must Integrate with LDAP for unified user authentication
		Must Integrate with LDAP groups for unified role definition
		Must Audit and securely store all user transactions
		Must Granular access controls to separate system maintenance functions from sensitive information access
		Must Secure access to the management console using HTTPS
		Must Secure remote maintenance access to the console using SSH
		Must Secure storage of local account passwords
		Must Security hardening measures to remove unnecessary services and network protocols to the DLP systems
	Reporting	Must Generate reports in PDF or CSV format
		Must Develop reports built around stakeholder requirements and schedule for email distribution
		Must Develop reports based on top (X) policy violations, senders, content type, protocol, etc.
		Must Build reports from GUI based on current view attributes (columns, content filters, view, etc.)
		Must Build detailed reports based on historical traffic/content analyzed by the DLP system
		Must Build detailed network traffic report for all network traffic analyzed by the DLP system
		Must Save report parameters for generating future reports
		Must Export historical records from all traffic/content analyzed by the DLP system the into an external system for analytical analysis
	System Platform for Network DLP	Must Purpose built appliance with option to operate as VMWare ESX virtual appliance
		Must be Turn-key installation and deployment
		DLP system, databases, and assets must be managed by a single department in an enterprise environment

		Single data-in-motion sensor must parse data up to 1 Gbps
		Single data-in-motion sensor must analysis and capture all traffic using for broadband network speeds of:
		Must Supports network attached storage
		System settings, cases, and incidents must be backed up and restored for system restoration
		Data-in-motion
		Must Identifies protocols based on protocol information, not port number (port agnostic)
		Must Identifies protocols operating on non-standard ports
		Must Performs IP address, protocol, content type recognition, content tagging, and rule processing on the wire (TCP Stack Level)
		Single sensor must analyze network traffic >200 Mbps without sampling traffic
		Single sensor must analyze different network segments using two capture ports at combined speeds >200Mbps
		Must supports alert generation to sender, sender's manager, policy reviewer, and additional e-mail recipients
		Must supports customized message content for alert notification e-mails
		Proactive blocking - data-in-motion
		Must interfaces with MTAs using X-header standard
		Must iInterfaces with web proxies using ICAP standard
		Single appliance must interface with web proxies with a combined bandwidth >100 Mbps
		Must upports analyzing SSL traffic by using man-in-the-middle compatible web proxies
		Must performs IP address, protocol, content type recognition, content tagging, and rule processing on the wire (TCP Stack Level)
		Must captures all traffic passing through MTA/web proxy for after the fact investigation
		Must supports the following actions for SMTP traffic: allow, block, reject, quarantine, encrypt
		Must supports the following actions for traffic processed by the web proxy: allow, block, attachment drop
		Data-at-rest
		Must support Windows and Samba files shares (CIFS)
		Must support Unix file shares (NFS)
		Must supports EMC Documentum

		Must supports SharePoint
		Must analyzes content, logs all file system information (owner, last modified date, creation date, etc.), creates a pointer to the target file, and removes the original file from the data-at-rest system
		Must performs content type recognition, and rule processing on the wire (TCP Stack Level)
		Must supports processing rules against data-at-rest scan tasks without having to re-scan the file repository
		Supports remediation of files violating policies (copy, delete, quarantine, encrypt) on CIFS Shares
		Signatures for sensitive documents must be created through scheduled scans and uploading through a web interface
		Must supports scanning desktop systems using an endpoint agent
	DLP Endpoint	Must Monitors content traversing across the endpoint by I/O channel (bus, Bluetooth, LPT, etc.)
		Must Monitors content traversing across the endpoint by IP address and protocol
		Must Monitors content traversing across the endpoint by application access
		Must Identify content based on content/document type
		Must Identify mass storage device by vendor specific identification numbers
		Must Identify content using regular expressions, key words, hash functions, and pattern matching.
		Must Identify content based on location
		Must Identify content using document fingerprint signatures
		Must Monitor transactions without notifying the end user across any of the egress methods mentioned above
		Must Notify the end user of a policy violation using a customizable pop-up message
		Must Capture content that violates a policy and store it in an evidence repository
		Must Blocks transactions across any of the egress methods mentioned above
		Must Blocks encrypted content from leaving the endpoint
		Must Create policies based on LDAP users and groups
		Must Enforce policies while the endpoint system is disconnected from the corporate network

		Endpoint agent must logs all violations and reports into the central database when a connection to the corporate network is established
		Rule override must be authorized using an override code issued from the security administrator
		Rule override must be authorized through end user justification
		Must Log all transactions to a central database
		Must deploy agent using central management console or common software deployment methods (GPO, SMS, etc.)
		Single endpoint server must manage up to 200k endpoints
		Must Protect endpoint agent from unauthorized removal or service stoppage regardless of local admin permissions
		Must Reinstall the agent or restart services in the event of unauthorized removal
		Must Encrypt/Quarantine/Monitor/Delete sensitive files found during endpoint discovery
		Must Encrypt sensitive files when copied to removable storage or network shares
		Must Block PDF Image writers
		Minimal use of system resources must be utilized for enforcing DLP policies
	Device Control key features	Device Control should be an Agent plug-in available for Windows and macOS versions.
		Controls what data can be copied to removable devices, or controls the devices themselves
		Should block devices completely or make them read-only.
		Provides protection for USB drives, smartphones, Bluetooth devices, and other removable media.
		Blocks executables on removable media from running allowing exceptions for required executables such as virus protection.
		Solution should allow policy creation to consisting of definitions, classifications, and rule sets in the management console
		Solution should allow for deployment of the policies to the endpoints.
		Collect incidents from the endpoints for monitoring and reporting.
		Device Control can monitor or block devices attached to enterprise-managed computers, allowing you to monitor and control their use in the distribution of sensitive information
		Devices such as smartphones, removable storage devices, Bluetooth devices, MP3 players, or plug-and-play devices

		should all be controlled
		The solution should provide:
		Device template to list device properties used to identify or group devices.
		Device group to list device templates grouped into a single template. Used to simplify rules while maintaining granularity.
		Device property such as bus type, vendor ID, or product ID that can be used to define a device.
		Device rule to define the action taken when a user attempts to use a device that has a matching device definition in the policy.
		The rule should be applied to the hardware, either at the device driver level or the file system level.
		The solution should allow for assigning device rules for specific end-users
		Should be bale to block removable storage devices or make them read-only
		The solution should allow defining Device class to have a collection of devices that have similar characteristics and can be managed in a similar manner.
		Device classes should allow the status Managed, Unmanaged, or Whitelisted where
		Managed device class status indicating that the devices in that class are managed by Device Control
		Unmanaged device class status indicating that the devices in that class are not managed by Device Control.
		Whitelisted device class status indicating that the devices in that class cannot be managed by Device Control because attempts to manage them can affect the managed computer, system health, or efficiency.
		The solution should allow below and The user should be notified of the action taken, as an option.
		Removable Storage Device Rule used to block or monitor removable storage devices, or set as read-only on Windows and Mac.
		Plug-and-play Device Rule Used to block or monitor plug-and- play devices for Windows and Mac for USB devices
		Removable Storage File Access Rule Used to block executables on plug-in devices from running on Windows for the file types: (.zip, .gz, .jar, .rar, and .cab) and executables (.bat, .bin, .cgi, .com, .cmd, .dll, .exe, .class, .sys, and .msi) and also allow customize the file extension definitions to add any

		file type required
		Fixed Hard Drive Rule Used to block or monitor fixed hard drives, or set as read-only, except for the boot or system partition.
		Should Support Citrix XenApp Device Rule Used to block Citrix devices mapped to shared desktop sessions for Windows
		TrueCrypt Device Rule Used to protect TrueCrypt devices. Can be used to block, monitor, or set to read-only.
	Administration	Solution should provide tool in the centralized management solution to provide overrides that allow users to perform functions that are normally prohibited
	Policy Bypass	When there is a legitimate business case, a use can request permission to access or transfer sensitive information The administrator can then grant permission for a limited time. When this is done, all sensitive information is monitored, rather than blocked, according to existing rules. Both the user and the system administrator receive messages about the bypass status when it is enabled and disabled (the user by a pop-up message, and the administrator by an event entry in the Operational Event List)
	Client uninstall	Client is protected from unauthorized removal.
		typically uninstalled by an administrator using central management console
		Should allow to be uninstalled in the field using the Microsoft Windows Add or Remove Programs function for situations where needed by the way of challenge/response key
		Should provide a Diagnostic Tool designed to aid troubleshooting Device COntrol Endpoint agent problems on Microsoft Windows endpoint computers
		The diagnostic tool should provide Displays all Plug and Play and removable devices currently connected to the computer and Displays all rules contained in the active policy, and the relevant policy definitions. Selecting a rule or definition displays the details.
	Drive Encryption	
	Drive Encryption Features	Drive Encryption delivers powerful encryption that protects data from unauthorized access, loss, and exposure on any system or disk when it is not in use provides multiple layers of defence against data loss with several integrated modules that address specific areas of risk.
		The suite provides protection for individual computers and

		roaming laptops with Basic Input Output System (BIOS) and Unified Extensible Firmware Interface (UEFI).
		Should support supports UEFI-based tablets
		Should provide a test tool to verify if the pre-boot environment will respond to the touch interface on tablets
		Must provide pre-boot environment for the user to first authenticate through
		the client system's operating system should load on successful authentication and gives access to normal system operation
		The disk encryption process is completely transparent to the user and has little impact on the computer's performance.
		Encryption begins only upon successful activation that is the system synchronizes with management solution and acquires user data, token data, and Pre-Boot theme data
		Also provides a way for offline activation
	Architecture	The solution should provide for a management solution that is scable and is centralized for all endpoints security solutions such as antimalware, device control, drive encryption, file and removable media encryption The Management solution allows management of Drive Encryption policies on client computer
		Allows to deploy and manage drive encryption software along with all endpoints security solutions such as antimalware, device control and file and removable media encryption
		Drive Encryption allows to acquire users through the Microsoft Active Directory (AD) or through the management solution
	Recovery	The recovery feature allows the end user to perform emergency recovery when the system fails to reboot or its Pre- Boot File System (PBFS) is corrupt.
		Support for self-encrypting drives allows centralized management of self-encrypting drives that conform to the Opal standard from Trusted Computing Group (TCG), including locking and unlocking, reporting, recovery, policy enforcement, and user management
		Trusted Platform Module (TPM) should support TPM 2.0 on Windows 8 and above UEFI systems in order to provide platform authentication without the need for Pre-Boot Authentication (PBA).
		Provides Self-recovery option that allows the user to reset a forgotten password by answering a set of security questions
		Provide option to enable or disable the administrator (system and user) recovery functionality on the client computer

		Provide Smartphone recovery as an option and available on Android and iOS smartphones
	File and Removable Media Protection	
	Features	Solution should deliver policy-enforced, automatic, and transparent encryption of files and folders stored or shared on PCs, file servers, cloud storage services, emails, and removable media such as USB drives, CD/DVDs, and ISO files. Provides support for Removable Media initialization for Mac client systems.
		Acts as a persistent encryption engine for operations performed through Windows File Explorer.
		When a file is encrypted, it remains encrypted even when:
		· The file is moved or copied to another location.
		· The file is moved out of an encrypted directory
		Architecture
		Centralized management — Provides support for deploying and managing
		User Personal Key — A unique encryption key is created for each user; administrators can reference “user personal key”
		Delegated administration through Role Based Key Management — Enables the logical separation of management between multiple administrators.
		Auditing of key management and policy assignments The key management and policy assignment-related actions performed by administrators are recorded in the Audit Log.
		Protection of data on removable media Enables encryption of removable media and access to encrypted content even on systems where client is not installed.
		Protection of data (including auditing and reporting) for cloud storage services - Enables encryption of sync folders on PCs for Dropbox, Box, Google Drive, and OneDrive.
		Network encryption — Enables secure sharing and collaboration on network shares
		User-initiated encryption of files and email attachments — Allows users to create and attach password-encrypted executable files that can be decrypted on systems where client is not installed.
		Auditing and reporting for USB removable media and CD/DVD/ISO events — Captures all end-user actions related to USB removable media and CD/DVD/ISO events.

		Provides performance benefits and leverages Intel® Advanced Encryption Standard Instructions (AES NI), resulting in additional performance improvements on systems with AES NI support.
		Should be bale to view summary information on FRP key usage and drill down to view the policies, users/groups, or systems/groups where they are used
		Provides Role Based Key Management to compartmentalize the administration of keys and permission sets for enhanced security by allowing you to define multiple key administrators based on permission sets defined by the Global Key Administrator
	Recovery	In case of forgotten password scenarios, end users should be provided with challenge and response mechanism to reset encrypted removable media and recover data from optical media. The recovery process can be used in both onsite and offsite scenarios and even on endpoints without the software installed
	Web Gateway (Proxy) Solution	
	Features	Must be deployed in high availability
		Must be able to manage on-prem users or off-prem users or both as hybrid approach
		Must be able to enforce Internet use policy
		Must have inbuilt capabilities like Anti-Virus, URL Filtering, SSL Inspection, zero-day anti malware, DLP
		Must provide full traffic visibility and control
		Inspect both HTTP & HTTPs traffic
		Block known threats at Gateway level
		Try to block unknown threats to the best of its capability with use of multi layered threat analysis engine's approach
		If the file still remains unknown / suspicious / gray, then Web Gateway must be able to integrate with the Sandbox solution mentioned above, forward the file for advanced analysis.
		Must use local and global techniques to analyze the nature and intent of all content and active code entering the network via the requested web pages
		Must have web filtering capability (Web categorization & web reputation)
		Must safeguard against unauthorized data leaving organization through bot infected machines

		Must provide data loss protection features to scan user- generated content on all key web protocols (HTTP, HTTPS, FTP)
		Must integrate with threat sharing solution and must check the file reputation with local threat intelligence before sending to the sandbox for advanced analysis
		Users when roaming must also apply the same set of web protection policies
		Must utilize the same endpoint agent as current to recognize if the user is on premise or off-premise. Based on user location, policies must be applied.
		Policy sharing for on-prem and off-prem users must be enabled so that no redundant policies are created based on user location
		Must be able to control applications at Layer 7
		Must support NTLM, RADIUS, AD/LDAP, eDirectory, cookie authentication, Kerberos, local user database authentication methods
		Must support single sign-on connectors for popular cloud- based applications
		Must be able to build custom reports
		Relevant alerts and reports must be able to send by email with automated setup
		Must be able to limit user's internet surfing based on time and or volume quota
		Must be able to control bandwidth
		Must be able to control file uploads or downloads based on categories or sites
		Must support caching
		Must support IPv4 & IPv6
		Must support multi-forest active directory environment like ours
		Must be able to detect and prevent malicious JavaScript and emulate the content for advanced detection
		Must support ICAP interface for external Network based DLP
		Must be able to distinguish between user-invoked downloaded files vs programmatic downloaded files
		Must be able to apply the traffic inspection engines for both inbound and outbound traffic
		Must be able to block peer to peer traffic

Annexures

Annexure A – RFP Schedule

Event No	Event Description	Timelines
1	Circulation / Advertisement of RFP	19th April 2023
2	Pre-Bid Meeting	28th April 2023
3	RFP Submission Date and Opening of Technical Proposal	10th May 2023
6	Technical Evaluation Result and Opening of Financial Proposal	Shall be intimated in due course of time
7	Announcement for Award of Contract	Shall be intimated in due course of time

*For site Visit Please Contact on **ddadmin@nitb.gov.pk** (preferably)
*Contact # 051-9265063

Annexure B – Submittal Requirements for Technical Proposal

S. No.	Description
1.	Cover Letter (on Bidder's Letter Head)
2.	Eligibility Requirements (Mandatory Requirements as mentioned in eligibility criteria)
3.	Responses to Sections 12 (Technical Evaluation Criteria & Bidder's Response) of this document.
4.	Executive Summary
5.	Company Profile (Profile, History, Addresses, Product / Solution Offerings, Contact Information, number of full-time employees, Customer in Pakistan etc.)
6.	Detailed Project Execution Plan / Work Breakdown Structure
7.	Training Methodology including Schedule & Plan
8.	Project Organization and Team Profiling **(Annexure-E)**
9.	Troubleshooting methodology
10.	System Service Support Plan
11.	Critical patches and updates
12.	Customer References and Relevancy
13.	Contact Details

Annexure C – Submittal Requirements for Financial Proposal

Bidders should submit financial cost as per table below. The cost of each Item/Equipment should cover all the allied costing and no other cost shall be entertained. All the cost should be one time and no recurring cost shall be allowed/accepted. Each item/equipment cost should also include training sessions along with free of cost certifications (for nominated users by NITB)

Lot#	Item/Equipment	QTY	Unit Price (US$)	GST/Local Taxes (%)	TOTAL GST/Local Taxes Amount (US$)	TOTAL PRICE (US$)

Annexure D – Client References:

Reference One (1)	Response
Company name	
Contact name and title	
Company address/phone	
Industry	
Installed Solutions	
Comments	
Reference Two (2)	Response
Company name	
Contact name and title	
Company address/phone	
Industry	
Installed Solutions	
Comments	
Reference Three (3)	Response
Company name	
Contact name and title	
Company address/phone	
Industry	
Installed Solutions	
Comments	

Annexure E – Management Group and Staff Profiling

Management Group				
Name of Staff	Areas of Expertise	Position Assigned	Full Time / Project based	Level of Involvement (%)

Proposed Staff				
Sr. #	Name of Staff	Areas of Expertise	Position Assigned	Level of Involvement (%)

Annexure F– Staff Resume

Proposed Position:	
Name of Staff:	CNIC #:
Date of Birth:	Age:
Nationality/Origin:	Number of Years with Bidder Company:
Educational Qualification:	
Relevant Work Experiences:	
Certifications:	
I am willing to work on the project as indicated in the deployment schedule and as required during the assignment period. I, the undersigned, certify that to the best of my knowledge and belief, this CV correctly describes me my qualification and my experience.	
Signature of Candidate	Signature of the Authorized Representative of the Company
Date:	
Email and Contact Number:	

Annexure G – Integrity Pact

__ [the Bidder] 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 Bidder] 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 Bidder] 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 Bidder] 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 Bidder] 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 Bidder] as aforesaid for the purpose of obtaining or inducing the procurement of any contract, right, interest, privilege or other obligation or benefit in whatsoever form from GoP.

For and On Behalf Of

_____

Signature: _____

Name: _____

NIC No: _____

Annexure H – Non-Disclosure Agreement

This Mutual Non-Disclosure Agreement ("Agreement") is made and entered into between National Information Technology Board (NITB), and [Bidder 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_____ 2022.
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:
- Business secrets.
- Financial information, including pricing.
- Technical information, including Installation, Commissioning, Configuration, Integration & Testing of Network Infrastructure.
- 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.

NITB	Company Name:
Address:	Address:
Name:	Name:
Signature:	Signature:
Title:	Title:
Date:	Date:

Annexure I – Technical Evaluation of Products / Services Strength

Bids evaluation shall be subject to 100% compliance to the following criteria for Bidder's qualification: Following table should be used for each Lot

Lot#	Item S.No.	Item Specification	Compliant	Non-Compliant