REPUBLIC OF THE PHILIPPINES
NATIONAL POWER CORPORATION
(Pambansang Korporasyon sa Elektrisidad)

BID DOCUMENTS

Name of Project : **TWO (2) YEARS OF LICENSE AND TECHNICAL SUPPORT OF THE EXISTING ANTIVIRUS**

Project Location : **NATIONAL POWER CORPORATION WAREHOUSE, GABRIEL Y. ITCHON BUILDING, SENATOR MIRIAM P. DEFENSOR-SANTIAGO AVENUE (FORMERLY BIR ROAD), CORNER QUEZON AVENUE, DILIMAN, QUEZON CITY-1100**

PR No. : **HO-IST25-005**

Contents :

SECTION I - INVITATION TO BID

SECTION II - INSTRUCTIONS TO BIDDERS

SECTION III - BID DATA SHEET

SECTION IV - GENERAL CONDITIONS OF CONTRACT

SECTION V - SPECIAL CONDITIONS OF CONTRACT

SECTION VI - TECHNICAL SPECIFICATIONS
PART I – Technical Specifications
PART II – Technical Data Sheets

SECTION VII - SCHEDULE OF REQUIREMENTS
(BID PRICE SCHEDULE)

SECTION VIII - BIDDING FORMS

Design and Development Department

SECTION I

INVITATION TO BID

National Power Corporation
INVITATION TO BID
PUBLIC BIDDING – BCS 2025-0382

1. The NATIONAL POWER CORPORATION (NPC), through its approved Corporate Budget of CY 2025 intends to apply the sum of **(Please see schedule below)** being the Approved Budget for the Contract (ABC) to payments under the contract. Bids received in excess of the ABC shall be automatically rejected at Bid opening.

PR Nos./PB Ref No. & Description	Similar Contracts	Pre-bid Conference	Bid Submission / Opening	ABC/ Amt. of Bid Docs
HO-IST25-005 / PB250729-RA00251 Two (2) Year of License and Technical Support of the Existing Antivirus	Provider / Distributor of an Endpoint Security Software (at least 600 clients)	16 July 2025 9:30 A.M.	29 July 2025 9:30 A.M.	₱ 4,300,000.00 / ₱ 5,000.00
HO-IST25-006 / PB250729-RA00252 Two (2) Years of License and Support Renewal of Existing Palo Alto Security Firewall	Supply, Delivery, Installation, Configuration and Testing of Network Security and Firewall			₱ 10,400,000.00 / ₱ 25,000.00
HO-IST25-007 / PB250729-RA00253 Two (2) Years of 500 MBPS or above Committed Information Rate Internet Gateway Service Connection for National Power Corporation	Provision of Internet Gateway Connection with speed of at least 500 MBPS (CIR)			₱ 1,596,000.00 / ₱ 5,000.00
Venue: Kañao Function Room, NPC Bldg. Diliman, Quezon City				

2. The NPC now invites bids for Items listed above. Delivery of the Goods is required **(see table below)** specified in the Technical Specifications. Bidders should have completed, within **(see table below)** from the date of submission and receipt of bids, a contract similar to the Project. The description of an eligible bidder is contained in the Bidding Documents, particularly, in Section II. (Instruction to Bidders).

PR No/s. / PB Ref No/s.	Delivery Period / Contract Duration	Relevant Period of SLCC reckoned from the date of submission & receipt of bids
HO-IST25-005	Thirty (30) Calendar Days / Two (2) Years	Five (5) Years
HO-IST25-006	Fifteen (15) Calendar Days / Two (2) Years	Five (5) Years
HO-IST25-007	Two (2) Years	Five (5) Years

3. Bidding will be conducted through open competitive bidding procedures using a non-discretionary "*pass/fail*" criterion as specified in the 2016 revised Implementing Rules and Regulations (IRR) of Republic Act (RA) No. 9184.

   Bidding is restricted to Filipino citizens/sole proprietorships, partnerships, or organizations with at least sixty percent (60%) interest or outstanding capital stock belonging to citizens of the Philippines, and to citizens or organizations of a country the laws or regulations of which grant similar rights or privileges to Filipino citizens, pursuant to RA 5183.

4. Prospective Bidders may obtain further information from National Power Corporation, Bids and Contracts Services Division and inspect the Bidding Documents at the address given below during office hours (8:00AM to 5:00PM), Monday to Friday.

5. A complete set of Bidding Documents may be acquired by interested Bidders from the given address and website(s) and upon payment of the applicable fee for the Bidding Documents, pursuant to the latest Guidelines issued by the GPPB. Payments via check, the payee should be: **NPC Bid Document Transactions**. *Bidding fee may be refunded in accordance with the guidelines based on the grounds provided under Section 41 of R.A. 9184 and its Revised IRR.*

6. The National Power Corporation will hold a Pre-Bid Conference on the date, time and venue stated above. Interested bidder/s is/are allowed to join and participate in the Pre-Bid Conference at the Kañao Room or virtually. However, those attending virtually shall assume the risk of any internet connectivity issues. Further, interested bidders are hereby informed of the following:

   a. Only a maximum of two (2) representatives from each bidder / company shall be allowed to participate
   b. Wearing of Face Masks is recommended but not required in view of Proclamation No. 297 S.2023 lifting the State of Public Health Emergency Throughout the Philippines
   c. The requirements herein stated including the medium of submission shall be subject to GPPB Resolution No. 09-2020 dated 07 May 2020
   d. The Guidelines on the Implementation of Early Procurement Activities (EPA) shall be subject to GPPB Circular No. 06-2019 dated 17 July 2019

7. Bids must be duly received by the BAC Secretariat through (i) manual submission at the office address indicated below; (ii) online or electronic submission before the specified time stated in the table above for opening of bids. Late bids shall not be accepted.

8. All Bids must be accompanied by a bid security in any of the acceptable forms and in the amount stated in **ITB** Clause 14.

9. Bid opening shall be in the Kañao Function Room, NPC Head Office, Diliman, Quezon City and/or via online platform to be announced by NPC. Bids will be opened in the presence of the bidders' representatives who choose to attend the activity.

10. The National Power Corporation reserves the right to reject any and all bids, declare a failure of bidding, or not award the contract at any time prior to contract award in accordance with Sections 35.6 and 41 of the 2016 revised IRR of R.A. No. 9184, without thereby incurring any liability to the affected bidder or bidders.

11. For further information, please refer to:

    Bids and Contracts Services Division,
    Logistics Department
    Gabriel Y. Itchon Building
    Senator Miriam P. Defensor-Santiago Ave. (formerly BIR Road)
    Cor. Quezon Ave., Diliman, Quezon City, 1100
    Tel Nos.: Tel Nos.: 8921-3541 local 5564/
    Email: bcsd@napocor.gov.ph /

12. You may visit the following websites:

    For downloading of Bidding Documents: https://www.napocor.gov.ph/bcsd/bids.php

LARRY I. SABELLINA
Vice President, MinGen and
Chairman, Bids and Awards Committee

SECTION II

INSTRUCTIONS TO BIDDERS

SECTION II – INSTRUCTIONS TO BIDDERS

TABLE OF CONTENTS

Clause No. **Title** **Page no.**

1. SCOPE OF BID 1
2. FUNDING INFORMATION 1
3. BIDDING REQUIREMENTS 1
4. CORRUPT, FRAUDULENT, COLLUSIVE, AND COERCIVE PRACTICES 1
5. ELIGIBLE BIDDERS 1
6. ORIGIN OF GOODS 2
7. SUBCONTRACTS 2
8. PRE-BID CONFERENCE 2
9. CLARIFICATION AND AMENDMENT OF BIDDING DOCUMENTS 3
10. DOCUMENTS COMPRISING THE BID: ELIGIBILITY AND TECHNICAL COMPONENTS 3
11. DOCUMENTS COMPRISING THE BID: FINANCIAL COMPONENT 3
12. BID PRICES 3
13. BID AND PAYMENT CURRENCIES 4
14. BID SECURITY 4
15. SEALING AND MARKING OF BIDS 4
16. DEADLINE FOR SUBMISSION OF BIDS 5
17. OPENING AND PRELIMINARY EXAMINATION OF BIDS 5
18. DOMESTIC PREFERENCE 5
19. DETAILED EVALUATION AND COMPARISON OF BIDS 5
20. POST-QUALIFICATION 6
21. SIGNING OF THE CONTRACT 6

SECTION II – INSTRUCTIONS TO BIDDERS

1. Scope of Bid

The **National Power Corporation (NPC** or **NAPOCOR)** wishes to receive Bids for the **TWO (2) YEARS OF LICENSE AND TECHNICAL SUPPORT OF THE EXISTING ANTIVIRUS,** with identification number **PR NO. HO-IST25-005.**

The Procurement Project (referred to herein as "Project") is composed of one (1) lot and will be awarded to one (1) Bidder in one complete contract, the details of which are described in Section VI (Technical Specifications).

2. Funding Information

2.1. The GOP through the source of funding as indicated below for CY 2025 - 2027 in the amount of **₱ 4,300,000.00.**

2.2. The source of funding is the Corporate Operating Budget of the National Power Corporation.

3. Bidding Requirements

The Bidding for the Project shall be governed by all the provisions of RA No. 9184 and its 2016 revised IRR, including its Generic Procurement Manuals and associated policies, rules and regulations as the primary source thereof, while the herein clauses shall serve as the secondary source thereof.

Any amendments made to the IRR and other GPPB issuances shall be applicable only to the ongoing posting, advertisement, or **IB** by the BAC through the issuance of a supplemental or bid bulletin.

The Bidder, by the act of submitting its Bid, shall be deemed to have verified and accepted the general requirements of this Project, including other factors that may affect the cost, duration and execution or implementation of the contract, project, or work and examine all instructions, forms, terms, and project requirements in the Bidding Documents.

4. Corrupt, Fraudulent, Collusive, and Coercive Practices

The Procuring Entity, as well as the Bidders and Suppliers, shall observe the highest standard of ethics during the procurement and execution of the contract. They or through an agent shall not engage in corrupt, fraudulent, collusive, coercive, and obstructive practices defined under Annex "I" of the 2016 revised IRR of RA No. 9184 or other integrity violations in competing for the Project.

5. Eligible Bidders

5.1. Only Bids of Bidders found to be legally, technically, and financially capable will be evaluated.

5.2. Foreign ownership exceeding those allowed under the rules may participate when citizens, corporations, or associations of a country, included in the list issued by the GPPB, the laws or regulations of which grant reciprocal rights or privileges to citizens, corporations, or associations of the Philippines.

The foreign bidder claiming eligibility by reason of their country's extension of reciprocal rights to Filipinos shall submit a certification from the relevant government office of their country stating that Filipinos are allowed to participate in their government procurement activities for the same item/product. The said certification shall be validated during the post-qualification of bidders.

5.3. Pursuant to Section 23.4.1.3 of the 2016 revised IRR of RA No.9184, the Bidder shall have an SLCC that is at least one (1) contract similar to the Project the value of which, adjusted to current prices using the PSA's CPI, must be at least equivalent to at least fifty percent (50%) of the ABC.

5.4. The Bidders shall comply with the eligibility criteria under Section 23.4.1 of the 2016 IRR of RA No. 9184.

6. Origin of Goods

There is no restriction on the origin of goods other than those prohibited by a decision of the UN Security Council taken under Chapter VII of the Charter of the UN, subject to Domestic Preference requirements under **ITB** Clause 18.

7. Subcontracts

7.1. The Bidder may subcontract portions of the Project to the extent allowed by the Procuring Entity as stated herein, but in no case more than twenty percent (20%) of the Project.

The portions of Project and the maximum percentage allowed to be subcontracted are indicated in the **BDS**, which shall not exceed twenty percent (20%) of the contracted Goods.

7.2. The Supplier may identify its subcontractor during the contract implementation stage. Subcontractors identified during the bidding may be changed during the implementation of this Contract. Subcontractors must submit the documentary requirements under Section 23.1 of the 2016 revised IRR of RA No. 9184 and comply with the eligibility criteria specified in **ITB** Clause 5 to the implementing or end-user unit.

7.3. Subcontracting of any portion of the Project does not relieve the Supplier of any liability or obligation under the Contract. The Supplier will be responsible for the acts, defaults, and negligence of any subcontractor, its agents, servants, or workmen as fully as if these were the Supplier's own acts, defaults, or negligence, or those of its agents, servants, or workmen.

8. Pre-Bid Conference

The Procuring Entity will hold a pre-bid conference for this Project on the specified date and time and either at its physical address and/or through videoconferencing/webcasting as indicated in paragraph 6 of the IB.

9. Clarification and Amendment of Bidding Documents

Prospective bidders may request for clarification on and/or interpretation of any part of the Bidding Documents. Such requests must be in writing and received by the Procuring Entity, either at its given address or through electronic mail indicated in the **IB**, at least ten (10) calendar days before the deadline set for the submission and receipt of Bids.

10. Documents comprising the Bid: Eligibility and Technical Components

10.1. The first envelope shall contain the eligibility and technical documents of the Bid as specified in Section VIII (NPCSF-GOODS-01 - Checklist of Technical and Financial Documents).

10.2. The Bidder's SLCC as indicated in **ITB** Clause 5.3 should have been completed within Five (5) Years prior to the deadline for the submission and receipt of bids.

10.3. If the eligibility requirements or statements, the bids, and all other documents for submission to the BAC are in foreign language other than English, it must be accompanied by a translation in English, which shall be authenticated by the appropriate Philippine foreign service establishment, post, or the equivalent office having jurisdiction over the foreign bidder's affairs in the Philippines. Similar to the required authentication above, for Contracting Parties to the Apostille Convention, only the translated documents shall be authenticated through an apostille pursuant to GPPB Resolution No. 13-2019 dated 23 May 2019. The English translation shall govern, for purposes of interpretation of the bid.

10.4. The Statement of the bidder's Single Largest Completed Contract (SLCC) (NPCSF-GOODS-03) and List of all Ongoing Government & Private Contracts Including Contracts Awarded but not yet Started (NPCSF-GOODS-02) shall comply with the documentary requirements specified in the **BDS.**

11. Documents comprising the Bid: Financial Component

11.1. The second bid envelope shall contain the financial documents for the Bid as specified in Section VIII (NPCSF-GOODS-01 - Checklist of Technical and Financial Documents).

11.2. If the Bidder claims preference as a Domestic Bidder or Domestic Entity, a certification issued by DTI shall be provided by the Bidder in accordance with Section 43.1.3 of the 2016 revised IRR of RA No. 9184.

11.3. Any bid exceeding the ABC indicated in paragraph 1 of the **IB** shall not be accepted.

11.4. For Foreign-funded Procurement, a ceiling may be applied to bid prices provided the conditions are met under Section 31.2 of the 2016 revised IRR of RA No. 9184.

12. Bid Prices

12.1. Prices indicated on the Price Schedule shall be entered separately in the following manner:

a. For Goods offered from within the Procuring Entity's country:

i. The price of the Goods quoted EXW (ex-works, ex-factory, ex-warehouse, ex-showroom, or off-the-shelf, as applicable);

ii. The cost of all customs duties and sales and other taxes already paid or payable;

iii. The cost of transportation, insurance, and other costs incidental to delivery of the Goods to their final destination; and

iv. The price of other (incidental) services, if any, listed in the **BDS.**

b. For Goods offered from abroad:

i. Unless otherwise stated in the **BDS**, the price of the Goods shall be quoted delivered duty paid (DDP) with the place of destination in the Philippines as specified in the **BDS**. In quoting the price, the Bidder shall be free to use transportation through carriers registered in any eligible country. Similarly, the Bidder may obtain insurance services from any eligible source country.

ii. The price of other (incidental) services, if any, as listed in the **BDS.**

13. Bid and Payment Currencies

13.1. For Goods that the Bidder will supply from outside the Philippines, the bid prices may be quoted in the local currency or tradeable currency accepted by the BSP at the discretion of the Bidder. However, for purposes of bid evaluation, Bids denominated in foreign currencies, shall be converted to Philippine currency based on the exchange rate as published in the BSP reference rate bulletin on the day of the bid opening.

13.2. Payment of the contract price shall be made in Philippine Pesos.

14. Bid Security

14.1. The Bidder shall submit a Bid Securing Declaration or any form of Bid Security in the amount indicated in the **BDS**, which shall be not less than the percentage of the ABC in accordance with the schedule in the **BDS.**

14.2. The Bid and bid security shall be valid for **One Hundred Twenty (120) calendar** days from the date of opening of bids. Any Bid not accompanied by an acceptable bid security shall be rejected by the Procuring Entity as non-responsive.

15. Sealing and Marking of Bids

Each Bidder shall submit Two (2) copies of the first and second components of its Bid, marked **Original** and photocopy. Only the original copy will be read and considered for the bid.

Any misplaced document outside of the **Original** copy will not be considered. The photocopy is ONLY FOR REFERENCE.

The Procuring Entity may request additional hard copies and/or electronic copies of the Bid. However, failure of the Bidders to comply with the said request shall not be a ground for disqualification.

If the Procuring Entity allows the submission of bids through online submission to the given website or any other electronic means, the Bidder shall submit an electronic copy of its Bid, which must be digitally signed. An electronic copy that cannot be opened or is corrupted shall be considered non-responsive and, thus, automatically disqualified.

Bidders must also comply with the Disclaimer and Data Privacy Notice specified in the **BDS**.

16. Deadline for Submission of Bids

16.1. The Bidders shall submit on the specified date and time and either at its physical address or through online submission as indicated in paragraph 7 of the **IB.**

17. Opening and Preliminary Examination of Bids

17.1. The BAC shall open the Bids in public at the time, on the date, and at the place specified in paragraph 9 of the **IB**. The Bidders' representatives who are present shall sign a register evidencing their attendance. In case videoconferencing, webcasting or other similar technologies will be used, attendance of participants shall likewise be recorded by the BAC Secretariat.

In case the Bids cannot be opened as scheduled due to justifiable reasons, the rescheduling requirements under Section 29 of the 2016 revised IRR of RA No. 9184 shall prevail.

17.2. The preliminary examination of bids shall be governed by Section 30 of the 2016 revised IRR of RA No. 9184.

18. Domestic Preference

18.1. The Procuring Entity will grant a margin of preference for the purpose of comparison of Bids in accordance with Section 43.1.2 of the 2016 revised IRR of RA No. 9184.

19. Detailed Evaluation and Comparison of Bids

19.1. The Procuring Entity's BAC shall immediately conduct a detailed evaluation of all Bids rated "*passed*," using non-discretionary pass/fail criteria. The BAC shall consider the conditions in the evaluation of Bids under Section 32.2 of the 2016 revised IRR of RA No. 9184.

19.2. If the Project allows partial bids, bidders may submit a proposal on any of the lots or items, and evaluation will be undertaken on a per lot or item basis, as the case maybe. In this case, the Bid Security as required by **ITB** Clause 14 shall be submitted for each lot or item separately.

19.3. The descriptions of the lots or items shall be indicated in **Section VI (Technical Specifications)**, although the ABCs of these lots or items are indicated in the **BDS** for purposes of the NFCC computation pursuant to Section 23.4.2.6 of the

2016 revised IRR of RA No. 9184. The NFCC must be sufficient for the total of the ABCs for all the lots or items participated in by the prospective Bidder.

19.4. The Project shall be awarded to one (1) Bidder in one complete contract.

19.5. Except for bidders submitting a committed Line of Credit from a Universal or Commercial Bank in lieu of its NFCC computation, all Bids must include the NFCC computation pursuant to Section 23.4.1.4 of the 2016 revised IRR of RA No. 9184, which must be sufficient for the total of the ABCs for all the lots or items participated in by the prospective Bidder. For bidders submitting the committed Line of Credit, it must be at least equal to ten percent (10%) of the ABCs for all the lots or items participated in by the prospective Bidder.

20. Post-Qualification

20.1. Within a non-extendible period of five (5) calendar days from receipt by the Bidder of the notice from the BAC that it submitted the Lowest Calculated Bid, the Bidder shall submit its latest income and business tax returns filed and paid through the BIR Electronic Filing and Payment System (eFPS) and other appropriate licenses and permits required by law and stated in the **BDS.**

21. Signing of the Contract

21.1. The documents required in Section 37.2 of the 2016 revised IRR of RA No. 9184 shall form part of the Contract. Additional Contract documents are indicated in the **BDS.**

SECTION III

BID DATA SHEETS

SECTION III - BID DATA SHEET

ITB Clause	
5.3	For this purpose, similar contracts shall refer to being a provider/distributor of an endpoint security software (at least 600 clients). The Single Largest Completed Contract (SLCC) as declared by the bidder shall be verified and validated to ascertain such completed contract. Hence, bidders must ensure access to sites of such projects/equipment to NPC representatives for verification and validation purposes during post-qualification process. It shall be a ground for disqualification, if verification and validation cannot be conducted for reasons attributable to the Bidder.
7.1	Subcontracting shall not be allowed for this particular procurement.
10.1	The prospective bidder shall submit a valid and updated Certificate of PhilGEPs Registration under Platinum Membership (all pages including the Annex A of the said Certificate). **Non-compliance shall be a ground for disqualification.**
10.4	The list of on-going contracts (Form No. NPCSF-GOODS-02) shall be supported by the following documents for each on-going contract to be submitted during **Post-Qualification**: 1. Contract/Purchase Order and/or Notice of Award 2. Certification coming from the project owner/client that the performance is satisfactory as of the bidding date The bidder shall declare in this form all his on-going government and private contracts including contracts where the bidder (either as individual or as a Joint Venture) is a partner in a Joint Venture agreement other than his current joint venture where he is a partner. Non declaration will be a ground for disqualification of bid.
	The Statement of the bidder's Single Largest Completed Contract (SLCC) similar to the contract to be bid (Form No. NPCSF-GOODS-03) shall be supported by the following documents to be submitted during **Bid Opening:** 1. Certificate of Acceptance; or Certificate of Completion; or Official Receipt (O.R); or Sales Invoice
	Any single bidder/s who already procured/secured the bidding documents but want to avail the Joint Venture Agreement (JVA) shall inform the BAC in writing prior to the bid opening for records and documentation purposes.

10.5	Bidders shall also submit the following requirements in their first envelope, Eligibility and Technical Component of their bid: 1. Data and Information to be submitted with the Proposal as specified in Clause TS-8.1 of Section VI - Technical Specifications; 2. Complete eligibility documents of the proposed sub-contractor, if any
12	The price of the Goods shall be quoted DDP Project Site or the applicable International Commercial Terms (INCOTERMS) for this Project.
14.1	The bid security shall be in the form of a Bid Securing Declaration, or any of the following forms and amounts: a) The amount of not less two percent (2%) of ABC, if bid security is in cash, cashier's/manager's check, bank draft/guarantee or irrevocable letter of credit; or b) The amount of not less than five percent (5%) of ABC, if bid security is in Surety Bond.
15.0	All bid submissions and related correspondences are confidential and for viewing only by the intended recipient/s. Any unauthorized access to review, reproduce, or disseminate the information contained therein is strictly prohibited. The National Power Corporation (NAPOCOR) does not guarantee the security of any information electronically transmitted. Bid submissions and related correspondences may contain personal and sensitive personal information, and are subject to the Data Privacy Act of 2012, its implementing rules, regulations and issuances of the National Privacy Commission of the Philippines ("Privacy Laws"). By viewing, using, storing, sharing and disposing (collectively "Processing"), such bids submissions and correspondences, you agree to comply with the Privacy Laws. By responding to correspondence, you consent to the Processing by NAPOCOR of the Personal Data contained in your submission/reply in accordance with NAPOCOR's Personal Data Privacy Policy which you can find at http://www.napocor.gov.ph. To report any privacy issue, contact the Data Privacy Officer at dpo@napocor.gov.ph. NAPOCOR is not liable for the proper and complete transmission of the information contained in bid submission/correspondences nor for any delay in its receipt.
19.3	The Goods are grouped together in one (1) lot and will be awarded to one (1) Bidder in one complete contract. Partial bid is not allowed. The Goods are grouped in a single lot and the lot shall not be divided into sub-lots for the purpose of bidding, evaluation, and contract award. The Bidders bid offer must be within the ABC of the lot.

	Bid offers that exceed the ABC of the lot or with incomplete price, shall be rejected.
19.5	If the Bidder opted to submit a Committed Line of Credit (CLC), the bidder must submit a granted credit line valid/effective at the date of bidding.
20.1	Additional documents to be submitted during Post-Qualification: a. Class A – Eligibility Documents listed on the Annex A of Certificate of PhilGEPs Registration under Platinum Membership pursuant to Section 34.3 of the Revised IRR of R.A. 9184 b. Contract/Purchase Order and/or Notice of Award for the contracts stated in the List of all Ongoing Government & Private Contracts Including Contracts Awarded but not yet Started (NPCSF-GOODS-02); c. Certification coming from the project owner/client that the performance is satisfactory as of the bidding date for all ongoing contracts stated in Form NPCSF-GOODS-02; d. Contract/Purchase Order for the contract stated in the Statement of the bidder's Single Largest Completed Contract (SLCC) similar to the contract to be bid (Form No. NPCSF-GOODS-03) e. Documents to be submitted during post-qualification process as specified in TS-8.2 of Section VI-Technical Specifications Manufacturer's brochures, manuals and other supporting documents of Software proposed by the bidders must comply with the technical specifications of such Software. It shall be a ground for disqualification if the submitted brochures, manuals and other supporting documents are determined not complying with the specifications during technical evaluation and post-qualification process. Software proposed by the winning bidder to be supplied, which were evaluated to be complying with the technical specifications, shall not be replaced and must be the same items to be delivered/installed/used during the contract implementation. Any proposed changes/replacement of said items may be allowed on meritorious reasons subject to validation and prior approval by NPC.
20.2	The licenses and permits relevant to the Project and the corresponding law requiring it as specified in the Technical Specifications, if any.
21.2	Notice to Proceed.

SECTION IV

GENERAL CONDITIONS OF CONTRACT

SECTION IV – GENERAL CONDITIONS OF CONTRACT

TABLE OF CONTENTS

Clause No. **Title** **Page no.**

1. SCOPE OF CONTRACT 1
2. ADVANCE PAYMENT AND TERMS OF PAYMENT 1
3. PERFORMANCE SECURITY 1
4. INSPECTION AND TESTS 1
5. WARRANTY 2
6. LIABILITY OF THE SUPPLIER 2

SECTION IV – GENERAL CONDITIONS OF CONTRACT

1. Scope of Contract

This Contract shall include all such items, although not specifically mentioned, that can be reasonably inferred as being required for its completion as if such items were expressly mentioned herein. All the provisions of RA No. 9184 and its 2016 revised IRR, including the Generic Procurement Manual, and associated issuances, constitute the primary source for the terms and conditions of the Contract, and thus, applicable in contract implementation. Herein clauses shall serve as the secondary source for the terms and conditions of the Contract.

This is without prejudice to Sections 74.1 and 74.2 of the 2016 revised IRR of RA No. 9184 allowing the GPPB to amend the IRR, which shall be applied to all procurement activities, the advertisement, posting, or invitation of which were issued after the effectivity of the said amendment.

Additional requirements for the completion of this Contract shall be provided in the **Special Conditions of Contract (SCC).**

2. Advance Payment and Terms of Payment

2.1. Advance payment of the contract amount is provided under Annex "D" of the revised 2016 IRR of RA No. 9184.

2.2. The Procuring Entity is allowed to determine the terms of payment on the partial or staggered delivery of the Goods procured, provided such partial payment shall correspond to the value of the goods delivered and accepted in accordance with prevailing accounting and auditing rules and regulations. The terms of payment are indicated in the **SCC**.

3. Performance Security

3.1. Within ten (10) calendar days from receipt of the Notice of Award by the Bidder from the Procuring Entity but in no case later than the signing of the Contract by both parties, the successful Bidder shall furnish the performance security in any of the forms prescribed in Section 39 of the 2016 revised IRR of RA No. 9184.

3.2. The performance bond to be posted by the Contractor must also comply with additional requirements specified in the **SCC.**

4. Inspection and Tests

The Procuring Entity or its representative shall have the right to inspect and/or to test the Goods to confirm their conformity to the Project specifications at no extra cost to the Procuring Entity in accordance with the Generic Procurement Manual. In addition to tests in the **SCC**, **Section VI (Technical Specifications)** shall specify what inspections and/or tests the Procuring Entity requires, and where they are to be conducted. The Procuring Entity shall notify the Supplier in writing, in a timely manner, of the identity of any representatives retained for these purposes.

All reasonable facilities and assistance for the inspection and testing of Goods, including access to drawings and production data, shall be provided by the Supplier to the authorized inspectors at no charge to the Procuring Entity.

5. Warranty

5.1 In order to assure that manufacturing defects shall be corrected by the Supplier, a warranty shall be required from the Supplier as provided under Section 62.1 of the 2016 revised IRR of RA No. 9184.

5.2 The Procuring Entity shall promptly notify the Supplier in writing of any claims arising under this warranty. Upon receipt of such notice, the Supplier shall, repair or replace the defective Goods or parts thereof without cost to the Procuring Entity, pursuant to the Generic Procurement Manual.

6. Liability of the Supplier

The Supplier's liability under this Contract shall be as provided by the laws of the Republic of the Philippines.

If the Supplier is a joint venture, all partners to the joint venture shall be jointly and severally liable to the Procuring Entity.

SECTION V

SPECIAL CONDITIONS OF CONTRACT

SECTION V – SPECIAL CONDITIONS OF CONTRACT

GCC Clause	
1.0	The Contractor shall perform the required services specified in Section VI – Technical Specifications upon commencement of the Contract.
2.2	Measurement and Terms of Payment is specified in Clause TS-10.0 of Section VI – Technical Specifications
3.2	1. The following must be indicated in the performance bond to be posted by the Contractor: i. Company Name ii. Correct amount of the Bond iii. Contract/Purchase Order Reference Number iv. Purpose of the Bond: "To guarantee the faithful performance of the Principal's obligation to undertake *(Contract/Purchase Order Description)* in accordance with the terms and conditions of *(Contract No. & Schedule/Purchase Order No.)* entered into by the parties." 2. The bond shall remain valid and effective until the duration of the contract *(should be specific date reckoned from the contract effectivity)* plus sixty (60) days after NPC's acceptance of the last delivery/final acceptance of the project. 3. In case of surety bond, any extension of the contract duration or delivery period granted to the CONTRACTOR shall be considered as given, and any modification of the contract shall be considered as authorized, as if with the expressed consent of the surety, provided that such extension or modifications falls within the effective period of the said surety bond. However, in the event that the extension of the contract duration or delivery schedule would be beyond the effective period of the surety bond first posted, it shall be the sole obligation of the CONTRACTOR to post an acceptable Performance Security within ten (10) calendar days after the contract duration/delivery period extension has been granted by NPC. 4. Other required conditions in addition to the standard policy terms issued by the Bonding Company: i. The bond is a penal bond, callable on demand and the entire amount thereof shall be forfeited in favor of the Obligee upon default of the Principal without the need to prove or to show grounds or reasons for demand for the sum specified therein; ii. The amount claimed by the Obligee under this bond shall be paid in full and shall never be subject to any adjustment by the Surety; iii. In case of claim, the Surety shall pay such claim within sixty (60) days from receipt by the Surety of the Obligee's notice of claim/demand letter notwithstanding any objection thereto by the Principal.
4	No further instructions

SECTION VI

TECHNICAL SPECIFICATIONS

PART I – TECHNICAL SPECIFICATIONS

PART II – TECHNICAL DATA SHEETS

SECTION VI

PART I

TECHNICAL SPECIFICATIONS

SECTION VI – TECHNICAL SPECIFICATIONS

PART I – TECHNICAL SPECIFICATIONS

TABLE OF CONTENTS

CLAUSE NO.	TITLE	PAGE NO.
TS-1.0	GENERAL	1
TS-2.0	SCOPE OF WORKS	1
TS-3.0	DELIVERY PERIOD AND LOCATION	1
TS-4.0	TECHNICAL REQUIREMENTS	1
TS-5.0	SERVICE LEVEL AGREEMENT (SLA)	12
TS-6.0	TRAINING	13
TS-6.0	ACCEPTANCE PLAN	13
TS-8.0	DATA AND DOCUMENTATION	13
TS-9.0	GUARANTEE	14
TS-10.0	MEASUREMENT OF PAYMENT	14

SECTION VI – TECHNICAL SPECIFICATIONS

TS-1.0 GENERAL

This specification outlines the requirements for the renewal of the license and technical support of the existing antivirus system of the National Power Corporation (NPC)

The National Power Corporation intends to avail of a two (2) years of license and technical support contract subscription of the existing antivirus with a practical, reliable, and comprehensive antivirus software solution that is easy to manage, cost-effective, and light on the computer system resources, which will commence immediately after the existing antivirus software contract expires on 31 August 2025.

The Supplier shall refer to the distributor/reseller of the antivirus system as specified in the Bid Documents.

TS-2.0 SCOPE OF WORKS

The Supplier's scope of work for the existing antivirus system shall cover the supply, delivery, installation, and configuration.

TS-3.0 DELIVERY PERIOD AND LOCATION

The delivery period shall be thirty (30) calendar days reckoned from the contract effectivity date stated in the Notice to Proceed.

The eligible Supplier shall deliver the proof of Antivirus Licenses and Technical Support subscription in the form of a Paper Subscription Certificate to the National Power Corporation Warehouse, Gabriel Y. Itchon Building, Senator Miriam P. Defensor-Santiago Avenue (formerly BIR Road), Corner Quezon Avenue, Diliman, Quezon City-1100.

Any and/or all expenses arising from the lack of knowledge or understanding regarding the site's existing conditions shall be the Supplier's responsibility, and NPC shall make no additional payment.

TS-4.0 TECHNICAL REQUIREMENTS

ITEM	DESCRIPTION	QUANTITY
1.	Endpoint Antivirus for Workstation Supported Platform Series: ▪ Windows 10, and 11	580 Clients

2.	File/Data Server Supported Platform Series: ▪ Windows Server 2016, 2019, 2022, and 2025	20 Clients

4.1 Integrated Management

All settings must be configured from a Central Dashboard without the need to access additional consoles.

4.2 Multi-Platform Management

Windows, Mac, and Linux machines must be managed from one console.

4.3 Updating Bandwidth Consumption

4.3.1 Updating of endpoints shall have configurable bandwidth settings, both software updating and threat definition updates.

4.3.2 The option must be given to set up a local cache updating server (on-premise) network environment to minimize extensive software engine updates.

4.3.3 An update management policy that contains the configuration of update schedules on managed endpoints must be created.

4.4 Deployment for the endpoint agent must support the following methodology:

4.4.1 Email setup link.

4.4.2 Setup via Active Directory (AD) Startup/Shutdown script

4.4.3 AD Login script.

4.4.4 Microsoft SCCM.

4.4.5 Include the endpoint agent installation in a gold image.

4.5 SIEM Integration

Must extract events and alert information from the Cloud Dashboard to a local SIEM.

4.6 API for Endpoint Management

4.6.1 APIs must be offered as RESTful HTTP endpoints over the public internet.

4.6.2 APIs must be capable of querying tenants, enumerating and managing endpoints and servers, and programming and managing alerts.

4.7 Role Management

4.7.1 The separation of estate management from different administrator logins must be allowed.

4.7.2 Must allow admins to assign predefined administrative roles to users who need access to the Admin Console.

4.7.3 Must be able to create custom roles and assign the products and access needed.

4.8 Microsoft AD Synchronization

4.8.1 The ability to only allow outbound synchronization of users/groups from the local Active Directory servers to the Cloud Dashboard for policy management must be enabled.

4.9 Policies

4.9.1 Selected policies should be able to be applied to either users or devices.

4.9.2 Policies must have the capability to be disabled automatically based on a scheduled time and date.

4.10 Enhanced Tamper Protection

4.10.1 The ability to prevent local administrative users or malicious processes from turning off endpoint protection must be enabled.

4.10.2 Must have the capability to prevent the following actions on the endpoint protection solution:

a. Stopping services from the Services UI
b. Kill services from the Task Manager UI
c. Change Service Configuration from the Services UI
d. Stop Services/edit service configuration from the command line
e. Uninstall
f. Reinstall
g. Kill processes from the Task Manager UI (desired)
h. Delete or modify protected files or folders
i. Delete or modify protected registry keys
j. Must be able to export Tamper Protection passwords in CSV or PDF formats.

4.11 Threat Protection

4.11.1 Must protect against multiple threats and provide a trusted and integrated approach to threat management at the endpoint.

4.11.2 Must protect endpoint systems against viruses, spyware, Trojans, rootkits, and worms on workstations and laptops, regardless of their nature or the concealment mechanisms used.

4.11.3 Must protect against threats related to executable files and document files containing active elements such as macros or scripts.

4.11.4 must protect against exploits resulting from the discovery (whether published or not) of security flaws in systems or software.

4.11.5 Must be able to 'lookup' files in real time to verify if they are malicious. This feature checks suspicious files against the latest malware in the vendor's Threat Intelligence database in the cloud.

4.11.6 Must be able to scan local files and network shares in real-time when the user tries to access them. Access must be denied unless the file is healthy.

4.11.7 Must have the capability to do real-time scanning of end-user Internet Access. It must monitor and classify Internet websites according to their level of risk and make this technology available to endpoint systems. A site known to host malicious code or phishing sites must

4.11.8 be proactively blocked by the solution to prevent any risk of infection or attack against a flaw of the browser used. The solution must conduct checks against a database of compromised websites that are constantly updated with new sites identified daily.

4.11.9 Must protect managed systems from malicious websites in real-time, whether end-users work within or outside the company's secure network - at home or through public Wi-Fi. All browsers on the market must be supported (Internet Explorer, Firefox, Safari, Opera, Chrome, etc.).

4.12 Anti-rootkit Detection:

A rootkit must be identified when reviewing an element without overloading the endpoint system. Rootkits must be proactively detected.

4.13 Suspicious Behavior Detection:

4.13.1 Must be able to protect against unidentified viruses and suspicious behavior.

4.13.2 Must have both pre-execution behavior analysis and runtime behavior analysis.

4.13.3 Must be able to identify and block malicious programs before execution.

4.13.4 Must be able to dynamically analyze the behavior of programs running on the system and detect and block activity that appears to be malicious. This may include changes to the registry that could allow a virus to run automatically when the computer is restarted.

4.13.5 Must protect against buffer overflow attacks.

4.14 Scanning

4.14.1 A scheduled scanner must be provided to run depending on the selected frequency or manually triggered through Windows Explorer to scan the specified directories (local, remote, or removable), with analysis parameters used, which may differ from those selected for real-time protection.

4.14.2 Must be able to scan archives such as zip, cab, etc., which can be enabled via policy settings.

4.15 Advanced Deep Learning Mechanism

4.15.1 Upon file execution, the system shall have light-speed scanning features that can conduct deep analysis and determine if a file is benign or malicious.

4.15.2 Must be able to prevent both known and never-seen-before malware; likewise, must be able to block malware before it executes.

4.15.3 Must protect the system even offline and will not rely on signatures.

4.15.4 Files must be classified as malicious, even potentially unwanted apps (PUA) or benign. Deep learning must also focus on Windows portable executables.

4.15.5 Able to perform new Zero-day threat scanning offline (without internet).

4.15.6 Must be Smarter - should be able to process data through multiple analysis layers, each layer making the model considerably more powerful.

4.15.7 Must be scalable - should be able to process significantly more input and can accurately predict threats while continuing to stay up-to-date.

4.15.8 Must Lighter - The model footprint shall be tiny, less than 20MB on the endpoint, with almost zero impact on performance.

4.15.9 The deep learning model shall be trialed and evaluated models end-to-end using advanced developed packages like Keras, TensorFlow, and Scikit-learn.

4.16 Exploit Prevention/Mitigation must detect and stop the following known exploits:

4.16.1 Enforcement of Data Execution Protection (DEP) prevents

4.16.2 Mandatory Address Space Layout Randomization (ASLR) prevents predictable code locations

4.16.3 Bottom-up ASLR improved code location randomization

4.16.4 Null Page (Null Dereference Protection) stops exploits that jump via page 0

4.16.5 Heap Spray Allocation reserving or pre-allocating commonly used memory addresses so they cannot be used to house payloads.

4.16.6 Dynamic Heap Spray stops attacks that spray suspicious sequences on the heap

4.16.7 Stack Pivot Stops abuse of the stack pointer

4.16.8 Stack Exec (MemProt) Stops attacker's code on the stack

4.16.9 Stack-based ROP Mitigations (Caller) Stops standard Return-Oriented Programming attacks

4.16.10 Branch-based ROP Mitigations (Hardware Augmented) Stops advanced Return-Oriented Programming attacks

4.16.11 Structured Exception Handler Overwrite Protection (SEHOP) Stops abuse of the exception handler

4.16.12 Import Address Table Access Filtering (IAF) (Hardware Augmented) Stops attackers that look at API addresses in the IAT

4.16.13 Load Library API calls Prevents loading of libraries from UNC paths

4.16.14 Reflective DLL Injection Prevents loading of a library from memory into a host process

4.16.15 Shellcode monitoring Detecting the adversarial deployment of shellcode involves multiple techniques to address things like fragmented shellcode, encrypted payloads, and null-free encoding

4.16.16 VBScript God Mode can detect the manipulation of the safe mode flag on VBScript in the web browser

4.16.17 WoW64 Must be able to prohibit the program code from directly switching from 32-bit to 64-bit mode (e.g., using ROP) while enabling the WoW64 layer to perform this transition.

4.16.18 Syscall Stops attackers that attempt to bypass security hooks

4.16.19 Hollow Process Protection Stops attacks that use legitimate processes to hide hostile code

4.16.20 DLL Hijacking Gives priority to system libraries for downloaded applications

4.16.21 Application Lockdown Will automatically terminate a protected application based on its behavior; for example, when an office application is leveraged to launch PowerShell, access the WMI, run a macro to install arbitrary code or manipulate critical system areas, the solution must block the malicious action – even when the attack doesn't spawn a child process.

4.16.22 Java Lockdown Prevents attacks that abuse Java to launch Windows executables

4.16.23 Squiblydoo AppLocker Bypass Prevents regsvr32 from running remote scripts and code

4.16.24 CVE-2013-5331 & CVE-2014-4113 via Metasploit In-memory payloads: Meterpreter & Mimikatz

4.16.25 APC Protection (Double Pulsar / AtomBombing) for Server

4.16.26 Process Privilege Escalation for Server

4.16.27 Dynamic Shellcode Protection Detects and blocks the behavior of stagers

4.16.28 EFS Guard Protection against Encrypting File System Attacks

4.16.29 CTF Guard Protects against a vulnerability in the "CTF" Windows component

4.16.30 ApiSetGuard Prevents applications from side-loading a malicious DLL posing as an ApiSet Stub DLL

4.17 Advanced Exploit Mitigation

Must be able to protect against a range of exploits or "active adversary" threats such as the following:

4.17.1 Credential Theft - Theft of passwords and hash information from memory, registry, or hard disk.

4.17.2 APC Violation - Attacks using Application Procedure Calls (APC) to run malicious codes.

4.17.3 Privilege Escalation - Attacks escalating a low-privilege process to higher privileges to access systems.

4.17.4 Code Cave Utilization - Malicious code inserted into another legitimate application.

4.17.5 Application Verifier Exploits - Attacks that exploit the application verifier to run unauthorized software at startup.

4.18 Malicious Traffic Detection (MTD)

Must detect communications between endpoint computers and command and control servers involved in a botnet or other malware attacks.

4.19 Intrusion Prevention System (IPS)

4.19.1 Must prevent malicious network traffic with packet inspection (IPS).

4.19.2 Must be able to scan traffic at the lowest level and block threats before harming the operating system or applications.

4.20 Anti-Ransomware Protection

4.20.1 The ability of the encrypted files to be rolled back to a pre-encrypted state must be met.

4.20.2 Anti-exploit and Ransomware protection do not need a Cloud Lookup to perform the detection.

4.20.3 When the Anti-crypto function suspects that a particular behavior is not in keeping with its intended process, the Data Recorder starts caching data. In contrast, the said behavior is closely reviewed to identify if the application is legitimate or if the activity is warranted. The maximum size of the data recorder is 100MB, and the Anti-crypto function caches files under 75.

4.20.4 The anti-crypto function shall look back at all the malicious file modifications made by that process and restore them to their original location.

4.20.5 Should a ransomware infection be managed to get in, detailed historical tracking of where the infection originated and how it propagated will be reported courtesy of the Threat Cases (RCA).

4.20.6 Must be able to protect from ransomware that encrypts the master boot record and attacks that wipe the hard disk.

4.21 AMSI Protection

4.21.1 Must be able to protect against malicious code (for example, PowerShell scripts) using the Microsoft Antimalware Scan Interface (AMSI).

4.21.2 Must be able to scan code forwarded via AMSI before it runs, and the applications used to run the code are notified of threats. If a threat is detected, an event is logged.

4.22 Data Loss Prevention (DLP)

4.22.1 Must be able to monitor and restrict the transfer of sensitive data files.

4.22.2 Must be able to create custom DLP policies or policies from templates.

4.22.3 DLP policy templates must be created to cover standard data protection for different regions.

4.23 Peripheral Control

4.23.1 Must have the capability to control and restrict removable mass storage devices (USB sticks, CD Rom, USB external hard drives, iPods, MP3 players, etc.), as well as connection devices (Wi-Fi, Bluetooth, Infrared, Modems, etc.).

4.23.2 The capability to add device exemptions must be either by Model ID or Instance ID.

4.24 Application Control

4.24.1 Must be able to limit the applications needed for specific user groups.

4.24.2 Must be able to detect and block application categories that may not be suitable for use in an enterprise environment.

4.24.3 Must have application categories for commonly used applications.

4.25 Web Control

4.25.1 Must be able to block risky downloads, protect against data loss, prevent users from accessing websites that are inappropriate for work, and generate logs of blocked visited sites.

4.25.2 Must have security options to configure access to ads, uncategorized sites, or dangerous downloads.

4.25.3 The administrator must be able to define "acceptable web usage" settings (defined by categories) to control the sites users are allowed to visit. Admin must have control access to websites identified and classified in their categories.

4.25.4 Must have a data loss protection option that allows the administrator to control access to web-based email and file downloads, with choices of blocking the data, allowing data sharing, or customizing this choice.

4.26 Windows Firewall Policy

4.26.1 Must be able to monitor and configure Windows Firewall on managed computers and servers using a Windows Firewall policy.

4.26.2 Must be able to apply the Windows Firewall policy to individual devices (computers or servers) or groups of devices.

4.27 Root Cause Analysis

4.27.1 Must have the capability to identify what happened, where a breach originated, what files were impacted, and provide guidance on how to strengthen an organization's security posture

4.27.2 You Must be able to record the chain of events after an infection has been detected, enabling you to determine the origin of the infection, any resulting damage to assets, potentially exposed data, and the chain of events leading up to the halting of the infection.

4.27.3 Shall summarize the event: What the exploit was discovered, where the beacon event occurred (an asset) when it occurred, and how the infection succeeded. E.g. "Outlook.exe."

4.27.4 recommendations to address the problem: Things to look for post-attack. For example, aside from files being restored from encrypted ones, check browser settings to ensure no vulnerabilities were created due to the infections.

4.27.5 Activity Record allows administrators to add notes to the case. All case-related notes will be listed in this column.

4.27.6 There are also buttons to enable the admin to modify the status of the case (New, In Progress, Closed) and to set priority (Low, Medium, High). When closing, the administrator can add notes and must confirm (via checkboxes) that remediation steps were taken: analyzed impact on files/assets and relevant environmental improvements were implemented.

4.27.7 Shall provide a tabular view of everything affected during the attack. Items can be filtered based on type — e.g., files, processes, and registry keys. The administrator can view information about each item, e.g., Filename (victim file or malware agent), process ID, and start/stop timestamp of the event.

4.27.8 Shall indicate the beginning of the root cause, charting out the series of events resulting from the attack as a collection of nodes. Each node contains specific information about files, processes, registry keys, etc., involved at that stage. The beacon event (marked with a blue dot) will be identified in the chain, but any events executed by the process identified as the beacon event will also be shown.

4.28 Advance System Clean

4.28.1 Must be able to trigger a deep clean upon any active detection from exploit or ransomware detection.

4.28.2 The next-gen endpoint shall provide advanced Clean detection of malware by looking for the following:

a. Files
b. Flagged as bad
c. File has been downloaded from the internet
d. Author's name/version information is missing from file properties, i.e., Impersonating a standard Windows system file. Reboot survivability is vigorously protected.
e. Un-common file extension used.
f. Contains PE structure anomalies and suggestions of obfuscation
g. Processes
h. Listening for incoming connections
i. Missing source executable file
j. No UI elements
k. Address Space Layout Randomization (ASLR) has been removed from the system.

4.29 Cloud Workload Discovery and Protection for Server

4.29.1 Must be able to discover and protect workloads on Amazon Web Services,

4.29.2 Microsoft Azure and Google Cloud Platform."

4.29.3 Must be able to connect to AWS and Azure accounts with the Server Protection admin console for enhanced management capabilities of Server Protection on AWS Elastic Compute Cloud (EC2) instances and Microsoft Azure Virtual Machines.

4.29.4 Must support AWS Auto Scaling.

4.29.5 Must be capable of Cloud Security Posture Management (monitor and secure cloud hosts, server-less functions, S3 buckets, and more)

4.30 Automatic Exclusion for Server

Must be able to automatically perform exclusion configuration after the Server Protection for Cloud installation.

4.31 Application Allows listing for Server

4.31.1 You Must have technology in the Server Protection agent that only allows approved applications to run on your servers to control what can run and modify files.

4.31.2 Must create trust between applications, control which application can update an app, and provide a data feed on trusted applications that automatically configures the product based on which applications the server has installed.

4.32 File Integrity Monitoring for Server

4.32.1 Must be able to assist customers who need to meet PCI-DSS compliance or those who would like to monitor system-critical files and registry keys for additional security.

4.32.2 Must be able to provide default rules that monitor changes to critical Windows system files as well as provide the ability to add additional monitoring locations and exclusions via policy.

4.32.3 Must be able to monitor files, folders, registry keys, and registry values.

4.33 Synchronized Security

Must be able to work with other security products of the vendor to share information and respond to incidents

4.33.1 Endpoint + Firewall:

a. Must automatically isolate infected endpoints on the public and local area networks.
b. Must be able to identify all apps on the network.
c. Must be able to link threats to individual users and computers.

4.33.2 Endpoint + Wireless Access Point must be able to restrict internet access for infected endpoints connected to Wi-Fi automatically.

TS-5.0 SERVICE LEVEL AGREEMENT (SLA)

5.1.1 Supplier shall provide 8x5 telephone, email support, and remote support on software application problems by qualified engineers and helpdesk support engineers, including the complete contact details of the Supplier's Support Group.

5.1.2 Helpdesk Support services shall cover support for technical problems, functional questions, and concerns about the hardware, equipment, and software.

5.1.3 A case number shall be assigned on every service request reported to the Supplier's Helpdesk Support Group and shall respond to NPC within four (4) hours after creating the case number.

5.1.4 Supplier shall provide quarterly on-site/remote support services to cover the product's health check within the warranty period.

5.1.6 NPC shall provide the Contractor's engineers and technicians access to the equipment it needs to fulfill the contracted support and services.

TS-6.0 TRAINING

The Supplier shall conduct a two (2) day refresher technical training course for at least seven (7) NPC personnel focusing on deployment, configuration, administration, maintenance, and basic troubleshooting. The supplier must ensure the training recipients are updated on all the technology's key practical aspects.

TS-6.0 ACCEPTANCE PLAN

6.1.1 The Supplier shall perform at his own expense all inspections required to ensure adequacy and conformance of the supplied Antivirus Solution to the requirements of the specifications and standards.

6.1.2 If the Antivirus Solution delivered fails to pass inspection, NPC may, in his judgment, direct the Supplier to make necessary replacements for the Antivirus and Internet Proxy Gateway as deemed appropriate.

6.1.3 A Certificate of Acceptance shall be issued by National Power Corporation only after all required installations and configurations have been done.

TS-8.0 DATA AND DOCUMENTATION

8.1 To be submitted with the bid.

8.1.1 Completely filled out Technical Data Sheets (TDS);

8.1.2 Service Level Agreement (SLA);

8.1.3 The Supplier must submit a Certificate of Distributor/Reseller from the Manufacturer issued to the Supplier, which is directly addressed to the BAC-NPC and indicates the PR/Reference number therein.

Note: The Certification from the Manufacturer/Principal shall be current and valid on the bid opening date as advertised.

8.2 To be submitted during post-qualification.

8.2.1 Manufacturer's Brochures/ Catalogues/ Drawings, which contain information/ data to support the Supplier's submitted and filled-out Technical Data Sheet;

8.2.2 Letter of Confirmation from the Manufacturer that a local agent or representative is available to provide "After Sales Service" to the supplied antivirus system during and after the warranty period. Name, address, and contact number shall be provided.

8.2.3 Certificate of Satisfactory Performance (CSP) from their customer (End-user) duly addressed to the Supplier that the supplied equipment of the same brand to be offered has performed satisfactorily in service.

All documents in Clause TS-8.2 shall be submitted to the Manager, ITSD, for evaluation and/or approval before the issuance of the acceptance certificate.

TS-9.0 GUARANTEE

The Supplier shall submit a Warranty Certificate for the two (2) year contract subscription period against factory defects/quality;

After the warranty period lapses, if no malfunction is found and/or repair works are pending, NPC shall release the warranty security/certificate.

TS-10.0 MEASUREMENT OF PAYMENT

The mode of payment shall be made annually for the two (2) years of license and technical support contract subscription of the existing antivirus. It shall constitute the full compensation as stated in Section VII, Schedule of Requirements, as follows:

1. Year 1, 50% of the total cost of the two (2) year contract subscription period.

2. Year 2, 50% of the total cost of the two (2) year contract subscription period.

NPC shall pay the Supplier within (30) days from the receipt of the complete supporting documents as required by NPC. The check will be prepared for payment to the Supplier subject to existing taxes.

SECTION VI

PART II

TECHNICAL DATA SHEETS

SECTION VI – TECHNICAL SPECIFICATIONS

PART II – TECHNICAL DATA SHEETS

TABLE OF CONTENTS

SECTION	DESCRIPTION	PAGE
1.0	TWO (2) YEARS OF LICENSE AND TECHNICAL SUPPORT OF THE E XISTING ANTIVIRUS	VI-TDS T VI

Name of Supplier: ____

Signature of Supplier: ________

SECTION VI - TECHNICAL SPECIFICATIONS

PART II – TECHNICAL DATASHEETS

TWO (2) YEARS OF LICENSE AND TECHNICAL SUPPORT OF THE EXISTING ANTIVIRUS

a. The Supplier shall complete this technical data sheet and submit the filled-up form with the technical proposal. The Supplier shall use continuation sheets as necessary for any additional information, keeping it in the format shown herein or reproducing it.

b. NPC reserves the right to reject Bids without proper and/or specific data and information as required herein.

c. The data required are technical features and characteristics of the Equipment/ component/material to be provided by the Supplier. Supplier's proposal shall at least be equal or superior to the requirements specified by NPC.

Name of Supplier: ______________________________

Signature of Supplier: ______________________________

1.0 TWO (2) YEARS OF LICENSE AND TECHNICAL SUPPORT OF THE EXISTING ANTIVIRUS

ITEM	DESCRIPTION	NPC'S REQUIREMENT	SUPPLIER'S DATA/ COMPLIANCE
1.1	580 Clients, Endpoint Antivirus for Workstation ▪ Supported Platform Series: Windows 10, and 11	To deliver	
1.2	20 Clients, File/Data Server ▪ Supported Platform Series: Windows Server 2016, 2019, 2022, and 2025	To deliver	
1.3	Integrated Management ▪ All settings must be configured from a Central Dashboard without the need to access additional consoles.	To deliver	
1.4	Multi-Platform Management ▪ Windows, Mac, and Linux machines must be managed from one management console	To deliver	
1.5	Updating Bandwidth Consumption ▪ Updating of endpoints shall have configurable bandwidth settings, both software updating and threat definition updates. ▪ Must be able to set up a local cache updating server (on-premise) network environment to minimize extensive software engine updates. ▪ Must have an Update Management Policy that contains the configuration of update schedules on managed endpoints.	To deliver	
1.6	Deployment for the endpoint agent must support the following methodology: ▪ Email setup link. ▪ Setup via Active Directory (AD) Startup/Shutdown script. ▪ AD Login script. ▪ Microsoft SCCM.	To deliver	

Name of Supplier: ______________________________

Signature of Supplier: ______________________________

ITEM	DESCRIPTION	NPC'S REQUIREMENT	SUPPLIER'S DATA/ COMPLIANCE
	▪ Include the endpoint agent installation in a gold image.		
1.7	SIEM Integration ▪ Must extract events and alert information from the Cloud Dashboard to a local SIEM.	To deliver	
1.8	API for Endpoint Management ▪ APIs must be offered as RESTful HTTP endpoints over the public internet. ▪ APIs must be able to query tenants, enumerate and manage endpoints and servers, and query alerts and manage them programmatically.	To deliver	
1.9	Role Management ▪ Must have the capability to allow the separation of estate management to different administrator logins. ▪ Must allow admins to assign predefined administrative roles to users who need access to the Admin Console. ▪ Must be able to create custom roles and assign the products and access needed.	To deliver	
1.10	Microsoft AD Synchronization ▪ Only outbound synchronization of users/groups from the local Active Directory servers to the Cloud Dashboard must be allowed for policy management.	To deliver	
1.11	Policies ▪ Selected policies should be able to be applied to either users or devices. ▪ Policies must have the capability to be disabled automatically based on a scheduled time and date.	To deliver	

Name of Supplier: ______________________________

Signature of Supplier: ______________________________

ITEM	DESCRIPTION	NPC'S REQUIREMENT	SUPPLIER'S DATA/ COMPLIANCE
1.12	Enhanced Tamper Protection ▪ Must prevent local administrative users or malicious processes from turning off the endpoint protection. ▪ Must have the capability to prevent the following actions on the endpoint protection solution: a. Stopping services from the Services UI b. Kill services from the Task Manager UI c. Change Service Configuration from the Services UI d. Stop Services/edit service configuration from the command line e. Uninstall f. Reinstall g. Kill processes from the Task Manager UI (desired) h. Delete or modify protected files or folders i. Delete or modify protected registry keys j. Must be able to export Tamper Protection passwords in CSV or PDF formats.	To deliver	
1.13	Threat Protection ▪ Must protect against multiple threats and provide a trusted and integrated approach to threat management at the endpoint. ▪ Must protect endpoint systems against viruses, spyware, Trojans, rootkits, and worms on workstations and laptops, regardless of their nature or the concealment mechanisms used. ▪ Must protect against threats to executable files and document files containing active elements such as macros or scripts. ▪ Must protect against exploits resulting from the discovery (whether published or not) of security flaws in systems or software. ▪ Must be able to 'lookup' files in real time to verify if they are malicious. This feature checks suspicious files against the latest malware in	To deliver	

Name of Supplier: ______________________________

Signature of Supplier: ______________________________

ITEM	DESCRIPTION	NPC'S REQUIREMENT	SUPPLIER'S DATA/ COMPLIANCE
	the vendor's Threat Intelligence database in the cloud. ▪ Must scan local files and network shares in real-time when the user tries to access them. Access must be denied unless the file is healthy. ▪ Must have the capability to scan end-user Internet Access in real-time. It must monitor and classify Internet websites according to their level of risk and make this technology available to endpoint systems. A site known to host malicious code or phishing sites must ▪ Be proactively blocked by the solution to prevent any risk of infection or attack against a flaw of the browser used. The solution must conduct checks against a database of compromised websites that are constantly updated with new sites identified daily. ▪ Must protect managed systems from malicious websites in real-time, whether end-users work within or outside the company's secure network - at home or through public Wi-Fi. All browsers on the market must be supported (Internet Explorer, Firefox, Safari, Opera, Chrome, etc.)		
1.14	Anti-rootkit Detection: ▪ Must identify a rootkit when reviewing an element without overloading the endpoint system. Rootkits must be proactively detected.	To deliver	
1.15	Suspicious Behavior Detection: ▪ Must be able to protect Against unidentified viruses and suspicious behavior. ▪ Must have both pre-execution behavior analysis and runtime behavior analysis. ▪ Must be able to identify and block malicious programs before execution.	To deliver	

Name of Supplier: ______________________

Signature of Supplier: ______________________

ITEM	DESCRIPTION	NPC'S REQUIREMENT	SUPPLIER'S DATA/ COMPLIANCE
	▪ Must be able to dynamically analyze the behavior of programs running on the system and detect and block activity that appears to be malicious. This may include changes to the registry that could allow a virus to run automatically when the computer is restarted. ▪ Must protect against buffer overflow attacks.		
1.16	Scanning ▪ Must provide a scheduled scanner to run depending on the selected frequency or manually trigger through Windows Explorer to scan the specified directories (local, remote, or removable), with analysis parameters used, which may differ from those selected for real-time protection. ▪ Must be able to scan archives such as zip, cab, etc., which can be enabled via policy settings.	To deliver	
1.17	Advanced Deep Learning mechanism ▪ Upon file execution, the system shall have light-speed scanning features that can conduct deep analysis and determine if a file is benign or malicious. ▪ Must be able to prevent both known and never-seen-before malware; likewise, must be able to block malware before it executes. ▪ Must protect the system even offline and will not rely on signatures. ▪ Must classify files as malicious, even potentially unwanted apps (PUA) or benign. Deep learning must also focus on Windows portable executables. ▪ Able to perform new Zero days' threat scanning offline (without internet). ▪ Must be Smarter - able to process data through multiple analysis layers, making the model considerably more powerful. ▪ Must be scalable - should be able to process significantly more input and can accurately	To deliver	

Name of Supplier: ______________________

Signature of Supplier: ______________________

ITEM	DESCRIPTION	NPC'S REQUIREMENT	SUPPLIER'S DATA/ COMPLIANCE
	predict threats while continuing to stay up-to-date. ▪ Must Lighter—The model footprint shall be tiny, less than 20MB on the endpoint, with almost zero impact on performance. ▪ The deep learning model shall be trialed and evaluated models end-to-end using advanced developed packages like Keras, TensorFlow, and Scikit-learn.		
1.18	Exploit Prevention/Mitigation must detect and stop the following known exploits: ▪ Enforcement of Data Execution Protection (DEP) prevents. ▪ Mandatory Address Space Layout Randomization (ASLR) prevents predictable code locations. ▪ Bottom-up ASLR improved code location randomization. ▪ Null Page (Null Dereference Protection) stops exploits that jump via page 0 ▪ Heap Spray Allocation reserving or pre-allocating commonly used memory addresses so they cannot be used to house payloads. ▪ Dynamic Heap Spray stops attacks that spray suspicious sequences on the heap ▪ Stack Pivot Stops abuse of the stack pointer. ▪ Stack Exec (MemProt): Stop the attacker's code on the stack. ▪ Stack-based ROP Mitigations (Caller) Stop standard Return-Oriented Programming attacks. ▪ Branch-based ROP Mitigations (Hardware Augmented) Stop advanced Return-Oriented Programming attacks ▪ Structured Exception Handler Overwrite Protection (SEHOP) Stops abuse of the exception handler.	To deliver	

Name of Supplier: ______________________________

Signature of Supplier: ______________________________

ITEM	DESCRIPTION	NPC'S REQUIREMENT	SUPPLIER'S DATA/ COMPLIANCE
	▪ ImpAddress Table Access Filtering (IAF) (Hardware Augmented) Stops attackers who look at API addresses in the IAT. ▪ LoadLibrary API calls Prevent the loading of libraries from UNC paths. ▪ Reflective DLL Injection Prevents loading of a library from memory into a host process. ▪ Shellcode monitoring Detecting the adversarial deployment of shellcode involves multiple techniques to address things like fragmented shellcode, encrypted payloads, and null-free encoding. ▪ VBScript God Mode can detect the manipulation of the safe mode flag on VBScript in the web browser. ▪ WoW64 Must be able to prohibit the program code from directly switching from 32-bit to 64-bit mode (e.g., using ROP) while enabling the WoW64 layer to perform this transition. ▪ Syscall Stops attackers that attempt to bypass security hooks. ▪ Hollow Process Protection Stops attacks that use legitimate processes to hide hostile code. ▪ DLL Hijacking Gives priority to system libraries for downloaded applications. ▪ Application Lockdown Will automatically terminate a protected application based on its behavior. For example, when an office application is leveraged to launch PowerShell, access the WMI, run a macro to install arbitrary code or manipulate critical system areas, the solution must block the malicious action—even when the attack doesn't spawn a child process. ▪ Java Lockdown Prevents attacks that abuse Java to launch Windows executables. ▪ Squiblydoo AppLocker Bypass Prevents regsvr32 from running remote scripts and code. ▪ CVE-2013-5331 & CVE-2014-4113 via Metasploit In-memory payloads: Meterpreter & Mimikatz.		

Name of Supplier: ______________________

Signature of Supplier: ______________________

ITEM	DESCRIPTION	NPC'S REQUIREMENT	SUPPLIER'S DATA/ COMPLIANCE
	▪ APC Protection (Double Pulsar/ AtomBombing) for Server. ▪ Process Privilege Escalation for Server. ▪ Dynamic Shellcode Protection Detects and blocks the behavior of stagers ▪ EFS Guard Protection against Encrypting File System attacks. ▪ CTF Guard Protects against a vulnerability in the "CTF" Windows component. ▪ ApiSetGuard Prevents applications from side-loading a malicious DLL posing as an ApiSet Stub DLL.		
1.19	Advanced Exploit Mitigation ▪ Must be able to protect against a range of exploits or "active adversary" threats such as the following: ▪ Credential Theft - Theft of passwords and hash information from memory, registry, or hard disk. ▪ APC Violation - Attacks using Application Procedure Calls (APC) to run malicious codes. ▪ Privilege Escalation - Attacks escalating a low-privilege process to higher privileges to access systems. ▪ Code Cave Utilization - Malicious code inserted into another legitimate application. ▪ Application Verifier Exploits - Attacks that exploit the application verifier to run unauthorized software at startup.	To deliver	
1.20	Malicious Traffic Detection (MTD) ▪ Must detect communications between endpoint computers and command and control servers involved in a botnet or other malware attacks.	To deliver	
1.21	Intrusion Prevention System (IPS) ▪ Must prevent malicious network traffic with packet inspection (IPS). ▪ Must be able to scan traffic at the lowest level and block threats before harming the operating system or applications.	To deliver	

Name of Supplier: ______________________

Signature of Supplier: ______________________

ITEM	DESCRIPTION	NPC'S REQUIREMENT	SUPPLIER'S DATA/ COMPLIANCE
1.22	Anti-Ransomware Protection ▪ The ability of the encrypted files to be rolled back to a pre-encrypted state must be required. ▪ Both Anti-exploit and Ransomware protection do not need to have a Cloud Lookup to perform the detection. ▪ When the Anti-crypto function suspects that particular behavior is not in keeping with its intended process, the Data Recorder starts caching data. In contrast, the said behavior is closely reviewed to identify if the application is legitimate or if the activity is warranted. The maximum size of the data recorder is 100MB, and the Anti-crypto function caches files under 75. ▪ The anti-crypto function shall look back at all the malicious file modifications made by that process and restore them to their original location. ▪ Should a ransomware infection be managed to get in, detailed historical tracking of where the infection originated and how it propagated will be reported courtesy of the Threat Cases (RCA). ▪ Must be able to protect from ransomware that encrypts the master boot record and attacks that wipe the hard disk.	To deliver	
1.23	AMSI Protection ▪ Must protect against malicious code (for example, PowerShell scripts) using the Microsoft Antimalware Scan Interface (AMSI). ▪ Must be able to scan code forwarded via AMSI before it runs, and the applications used to run the code are notified of threats. If a threat is detected, an event is logged.	To deliver	
1.24	Data Loss Prevention (DLP) ▪ Must be able to monitor and restrict the transfer of sensitive data files.	To deliver	

Name of Supplier: ______________________________

Signature of Supplier: ______________________________

ITEM	DESCRIPTION	NPC'S REQUIREMENT	SUPPLIER'S DATA/ COMPLIANCE
	▪ Must be able to create custom DLP policies or policies from templates. ▪ DLP policy templates must cover standard data protection for different regions.		
1.25	Peripheral Control ▪ Must control and restrict removable mass storage devices (USB sticks, CD Rom, USB external hard drives, iPods, MP3 players, etc.) and connection devices (Wi-Fi, Bluetooth, Infrared, Modems, etc.). ▪ Must be able to add device exemptions either by Model ID or Instance ID.	To deliver	
1.26	Application Control ▪ Must be able to limit the applications needed for specific user groups. ▪ Must be able to detect and block application categories that may not be suitable for use in an enterprise environment. ▪ Must have application categories for commonly used applications.	To deliver	
1.27	Web Control ▪ Must be able to block risky downloads, protect against data loss, and prevent users from accessing ▪ websites that are inappropriate for work and generate logs of blocked visited sites. ▪ Must have security options to configure access to ads, uncategorized sites, or dangerous downloads. ▪ Must allow the administrator to define "acceptable web usage" settings (defined by categories) to control the sites on which users are allowed to visit. Admin must have control	To deliver	

Name of Supplier: ______________________________

Signature of Supplier: ______________________________

ITEM	DESCRIPTION	NPC'S REQUIREMENT	SUPPLIER'S DATA/ COMPLIANCE
	access to websites identified and classified in their categories. ▪ There must be a data loss protection option that allows the administrator to control access to web-based email and file downloads, blocking the data, allowing data sharing, or customizing this choice.		
1.28	Windows Firewall Policy ▪ Must be able to monitor and configure Windows Firewall on managed computers and servers using a Windows Firewall policy. ▪ Must be able to apply the Windows Firewall policy to individual devices (computers or servers) or groups of devices.	To deliver	
1.29	Root Cause Analysis ▪ Must have the capability to identify what happened, where a breach originated, and what files were impacted, and provide guidance on how to strengthen an organization's security posture ▪ Must be able to record the chain of events after an infection has been detected, which enables you to determine the origin of the infection, any resulting damage to assets, potentially exposed data, and the chain of events leading up to the halting of the infection. ▪ Shall summarize the event: What the exploit was discovered, where the beacon event occurred (an asset) when it happened, and how the infection succeeded. E.g. "Outlook.exe." ▪ Shall provide recommendations to address the problem: Things to look for post-attack. For example, aside from files being restored from encrypted ones, check browser settings to ensure no vulnerabilities were created due to the infections.	To deliver	

Name of Supplier: ______________________

Signature of Supplier: ______________________

ITEM	DESCRIPTION	NPC'S REQUIREMENT	SUPPLIER'S DATA/ COMPLIANCE
	▪ Activity Record allows administrators to add notes to the case. All case-related notes will be listed in this column. ▪ There are also buttons to enable the admin to modify the status of the case (New, In Progress, Closed) and to set priority (Low, Medium, High). When closing, the administrator can add notes and must confirm (via checkboxes) that remediation steps were taken: analyzed impact on files/assets and relevant environmental improvements were implemented. ▪ Shall provide a tabular view of everything affected during the attack. Items can be filtered based on type — e.g., files, processes, and registry keys. The administrator can view information about each item, e.g., Filename (victim file or malware agent), process ID, and start/stop timestamp of the event. ▪ Shall indicate the beginning of the root cause, charting out the series of events resulting from the attack as a collection of nodes. Each node contains specific information about files, processes, registry keys, etc., involved at that stage. The beacon event (marked with a blue dot) will be identified in the chain, but any events executed by the process identified as the beacon event will also be shown.		
1.30	Advance System Clean ▪ Must be able to trigger a deep clean upon any active detection from exploit or ransomware detection. ▪ The next-gen endpoint shall provide advanced Clean detection of malware by looking for the following: a. Files. b. Flagged as bad. c. File has been downloaded from the internet.	To deliver	

Name of Supplier: ________________________

Signature of Supplier: ________________________

ITEM	DESCRIPTION	NPC'S REQUIREMENT	SUPPLIER'S DATA/ COMPLIANCE
	d. Author's name/version information is missing from file properties, i.e., Impersonating a standard Windows system file. Reboot survivability is vigorously protected. e. Un-common file extension used. f. Contains PE structure anomalies and suggestions of obfuscation. g. Processes. h. Listening for incoming connections i. Missing source executable file j. There are no UI elements. k. Address Space Layout Randomization (ASLR) has been removed from the system.		
1.31	Cloud Workload Discovery and Protection for Server ▪ Must be able to discover and protect workloads on Amazon Web Services, ▪ Microsoft Azure and Google Cloud Platform." ▪ Must be able to connect to AWS and Azure accounts with the Server Protection admin console for enhanced management capabilities of Server Protection on AWS Elastic Compute Cloud (EC2) instances and Microsoft Azure Virtual Machines. ▪ Must support AWS Auto Scaling. ▪ Must be capable of Cloud Security Posture Management (monitor and secure cloud hosts, server-less functions, S3 buckets, and more)	To deliver	
1.32	Automatic Exclusion for Server ▪ Must be able to automatically perform exclusion configuration after installing the Server Protection for Cloud installation.	To deliver	
1.33	Application Allows listing for Server. ▪ Must have technology in the Server Protection agent that only allows approved applications to	To deliver	

Name of Supplier: ______________________

Signature of Supplier: ______________________

ITEM	DESCRIPTION	NPC'S REQUIREMENT	SUPPLIER'S DATA/ COMPLIANCE
	run on your servers to control what can run and modify files. ▪ Must be able to create trust between applications, control which application can update an app, and provide a data feed on trusted applications that automatically configures the product based on which applications the server has installed.		
1.34	File Integrity Monitoring for Server ▪ Must be able to assist customers who need to meet PCI-DSS compliance or those who would like to monitor system-critical files and registry keys for additional security. ▪ Must be able to provide default rules that monitor changes to critical Windows system files as well as provide the ability to add additional monitoring locations and exclusions via policy. ▪ Must be able to monitor files, folders, registry keys, and registry values.	To deliver	
1.35	Synchronized Security Must be able to work with other security products of the vendor to share information and respond to incidents: • Endpoint + Firewall: a. Must automatically isolate infected endpoints on the public and local area networks. b. Must be able to identify all apps on The network. c. Must be able to link threats to individual users and computers.	To deliver	

Name of Supplier: ______________________

Signature of Supplier: ______________________

ITEM	DESCRIPTION	NPC'S REQUIREMENT	SUPPLIER'S DATA/ COMPLIANCE
	▪ Endpoint + Wireless Access Point must be able to restrict internet access for infected endpoints connected to Wi-Fi automatically.		
1.36	The Supplier shall conduct a two (2) day refresher technical training course for at least seven (7) NPC personnel focusing on deployment, configuration, administration, maintenance, and basic troubleshooting. The supplier must ensure the training recipients are updated on all the technology's key practical aspects.	To deliver	

Name of Supplier: ____________________

Signature of Supplier: ____________________

SECTION VII

SCHEDULE OF REQUIREMENTS

SECTION VII - SCHEDULE OF REQUIREMENTS
(BID PRICE SCHEDULE)
TWO (2) YEARS OF LICENSE AND TECHNICAL SUPPORT OF THE EXISTING ANTIVIRUS
PR. NO. HO-IST25-005

ITEM NO.	DESCRIPTION OF WORK OR MATERIALS	QTY/ UNIT	* CODE	UNIT PRICE FOR GOODS AND RELATED SERVICES TO BE SUPPLIED AND DELIVERED					TOTAL PRICE
				Unit Price of Goods Delivered up to Philippine Port +(Phil. Peso)	Import Duties & other Levies Imposed by Phil. Govt. (Phil. Peso)	Value Added Tax and other Taxes Imposed by Phil. Govt. (Phil. Peso)	Local Transport from Port to Delivery Site <(Phil. Peso)	Unit Price of Goods or Services >(Phil. Peso)	Local Currency (Phil. Peso) ((E+F+G+H+I) x C)
(A)	(B)	(C)	(D)	(E)	(F)	(G)	(H)	(I)	(J)
1	Two (2) years of license and technical support of the existing antivirus system, including all other works and services as specified in the Technical Specifications. a) A total of 580 clients of Endpoint antivirus for workstation with supported platform series: Windows 10 & 11 b) A total of 20 clients of File/data server with supported platform series: Windows 2016, 2019, 2022 & 2025 -	1 Lot							
TOTAL				AMOUNT IN WORDS:					AMOUNT IN FIGURES:

Notes:

- * Bidders shall enter a code representing the Country of Origin of all imported equipment, materials and accessories.
- + Cost of equipment, freight, insurance, etc. up to Phil. port of entry.
- < Unit Price for Local Transportation, insurance and other local costs incidental to delivery of the goods from the Phil port of entry to final delivery site.
- > Unit Price for Local Transportation, insurance and other local costs incidental to delivery of the goods from local source to final delivery site.

Code	Country of Origin

Delivery: Refer to Part I - Technical Specification, Clause TS-3.0 for the delivery location.

Name of Supplier

Name and Signature of Authorized Representative

Designation

SECTION VIII

BIDDING FORMS

SECTION VIII – BIDDING FORMS

TABLE OF CONTENTS

NPCSF-GOODS-01 - Checklist of Technical and Financial Envelope Requirements for Bidders

NPCSF-GOODS-02 - List of all Ongoing Government & Private Contracts Including Contracts Awarded but not yet Started

NPCSF-GOODS-03 - Statement of the bidder's Single Largest Completed Contract (SLCC) similar to the contract to be bid

NPCSF-GOODS-04 - Computation of Net Financial Contracting Capacity (NFCC)

NPCSF-GOODS-05 - Joint Venture Agreement

NPCSF-GOODS-06a - Form of Bid Security : Bank Guarantee

NPCSF-GOODS-06b - Form of Bid Security : Surety Bond

NPCSF-GOODS-06c - Bid Securing Declaration Form

NPCSF-GOODS-07 - Omnibus Sworn Statement (Revised)

NPCSF-GOODS-08 - Bid Letter

Sample Form - Bank Guarantee Form for Advance Payment

Sample Form - Certification from DTI as Domestic Bidder

Standard Form No: NPCSF-GOODS-01

Checklist of Technical & Financial Envelope Requirements for Bidders

A. THE 1ST ENVELOPE (TECHNICAL COMPONENT) SHALL CONTAIN THE FOLLOWING:

1. *ELIGIBILITY DOCUMENTS*

a. *(CLASS A)*

➢ PhilGEPs Certificate of Registration and Membership under Platinum Category (all pages) in accordance with Section 8.5.2 of the Revised IRR of RA. 9184;

Note: The failure by the prospective bidder to update its Certificate with the current and updated Class "A" eligibility documents shall result in the automatic suspension of the validity of its Certificate until such time that all of the expired Class "A" eligibility documents has been updated

➢ Statement of all its ongoing government and private contracts if any, whether similar or not similar in nature and complexity to the contract to be bid *(NPCSF-GOODS-02)*

➢ The Statement of the bidder's Single Largest Completed Contract (SLCC) similar to the contract to be bid, and whose value, adjusted to current prices using the Philippine Statistics Authority (PSA) consumer price index, must be at least 50% of the ABC *(NPCSF-GOODS-03)* complete with the following supporting documents:

1. Certificate of Acceptance; or Certificate of Completion; or Official Receipt (O.R); or Sales Invoice

(The Single Largest Completed Contract (SLCC) as declared by the bidder shall be verified and validated to ascertain such completed contract. Hence, bidders must ensure access to sites of such projects/equipment to NPC representatives for verification and validation purposes during post-qualification process.
It shall be a ground for disqualification, if verification and validation cannot be conducted for reasons attributable to the Bidder.)

➢ Duly signed computation of its Net Financial Contracting Capacity (NFCC) at least equal to the ABC (NPCSF-GOODS-04) or a Committed Line of Credit (CLC) at least equal to ten percent (10%) of the ABC, issued by a Universal or Commercial Bank; If the Bidder opted to submit a Committed Line of Credit (CLC), the bidder must submit a granted credit line valid/effective at the date of bidding.

b. *(CLASS B)*

➢ For Joint Venture (if applicable), any of the following:

- Valid Joint Venture Agreement *(NPCSF-GOODS-05)*

OR

- Notarized statements from all the potential joint venture partners stating that they will enter into and abide by the provisions of the JVA, if awarded the contract

➢ Certification from the relevant government office of their country stating that Filipinos are allowed to participate in their government procurement activities for the same item/product *(For foreign bidders claiming eligibility by reason of their country's extension of reciprocal rights to Filipinos)*

This Checklist of Requirements shall be provided to prospective suppliers/contractors including all forms. Suppliers/contractors are encouraged to consult this checklist before submitting their proposals on the deadline for the submission and receipt of offers.

Standard Form No: NPCSF-GOODS-01

2. Technical Documents

- ➢ Bid Security, any one of the following:
  - Bid Securing Declaration (NPCSF-GOODS-06c)

    OR
  - Cash or Cashier's/Manager's check issued by a Universal or Commercial Bank – *2% of ABC;*

    OR
  - Bank draft/guarantee or irrevocable letter of credit issued by a Universal or Commercial Bank: *(NPCSF-GOODS-06a) - 2% of ABC;*

    OR
  - Surety Bond callable upon demand issued by a reputable surety or insurance company *(NPCSF-GOODS-06b) - 5% of ABC, with*
    - ▪ Certification from the Insurance Commission as authorized company to issue surety
- ➢ Duly signed, completely filled-out and notarized Omnibus Sworn statement (Revised) (NPCSF-GOODS-07), complete with the following attachments:
  - For Sole Proprietorship:
    - ▪ Special Power of Attorney
  - For Partnership/Corporation/Cooperative/Joint Venture:
    - ▪ Document showing proof of authorization (e.g., duly notarized Secretary's Certificate, Board/Partnership Resolution, or Special Power of Attorney, whichever is applicable)
- ➢ Documents to be submitted with the Proposal as specified in Clause TS-8.1 of Section VI - Technical Specifications;

B. THE 2ND ENVELOPE (FINANCIAL COMPONENT) SHALL CONTAIN THE FOLLOWING:

- ➢ Duly signed Bid Letter indicating the total bid amount in accordance with the prescribed form *(NPCSF-GOODS-08)*
- ➢ Duly signed and completely filled-out Schedule of Requirement *(Section VII)* indicating the unit and total prices per item and the total amount in the prescribed Price Schedule form.
- ➢ For Domestic Bidder claiming for domestic preference:
  - Letter address to the BAC claiming for preference
  - Certification from DTI as Domestic Bidder in accordance with the prescribed forms provided

Standard Form No: NPCSF-GOODS-01

CONDITIONS:

1. *Each Bidder shall submit Two (2) copies of the first and second components of its Bid, marked Original and photocopy. Only the original copy will be read and considered for the bid. Any misplaced document outside of the Original copy will not be considered. The photocopy is ONLY FOR REFERENCE. NPC may request additional hard copies and/or electronic copies of the Bid. However, failure of the Bidders to comply with the said request shall not be a ground for disqualification.*

2. *In the case of foreign bidders, the eligibility requirements under Class "A" Documents (except for Tax Clearance) may be substituted by the appropriate equivalent documents, if any, issued by the country of the foreign bidder concerned. The eligibility requirements or statements, the bids, and all other documents to be submitted to the BAC must be in English. If the eligibility requirements or statements, the bids, and all other documents submitted to the BAC are in foreign language other than English, it must be accompanied by a translation of the documents in English. The documents shall be translated by the relevant foreign government agency, the foreign government agency authorized to translate documents, or a registered translator in the foreign bidder's country; and shall be authenticated by the appropriate Philippine foreign service establishment/post or the equivalent office having jurisdiction over the foreign bidder's affairs in the Philippines.*

   These documents shall be accompanied by a Sworn Statement in a form prescribed by the GPPB stating that the documents submitted are complete and authentic copies of the original, and all statements and information provided therein are true and correct. Upon receipt of the said documents, the PhilGEPS shall process the same in accordance with the guidelines on the Government of the Philippines – Official Merchants Registry (GoP-OMR).

3. *A Bidder not submitting bid for reason that his cost estimate is higher than the ABC, is required to submit his letter of non-participation/regret supported by corresponding detailed estimates. Failure to submit the two (2) documents shall be understood as acts that tend to defeat the purpose of public bidding without valid reason as stated under Section 69.1.(i) of the revised IRR of R.A. 9184.*

This Checklist of Requirements shall be provided to prospective suppliers/contractors including all forms. Suppliers/contractors are encouraged to consult this checklist before submitting their proposals on the deadline for the submission and receipt of offers.

Standard Form Number: NPCSF-GOODS-02

List of All Ongoing Government and Private Contracts Including Contract Awarded But Not Yet Started

Business Name : ______________________
Business Address : ______________________

Name of Contract/ Project Cost	a. Owner's Name b. Address c. Telephone Nos.	Nature of Work	Bidder's Role		a. Date Awarded b. Date Started c. Date of Completion or Contract Duration/ Date of Delivery	Value of Outstanding Works / Undelivered Portion
			Description	%		
Government						
Private						
					Total Cost	

The bidder shall declare in this form all his on-going government and private contracts including contracts where the bidder (either as individual or as a Joint Venture) is a partner in a Joint Venture agreement other than his current joint venture where he is a partner. Non declaration will be a ground for disqualification of bid.

Note : This statement shall be supported with the following documents for all the contract(s) stated above which shall be submitted during Post-qualification:

1. Contract/Purchase Order and/or Notice of Award
2. Certification coming from the project owner/client that the performance is satisfactory as of the bidding date.

Submitted by : ______________________
(Printed Name & Signature)

Designation : ______________________
Date : ______________________

Standard Form Number: NPCSF-GOODS-03

The Statement of the bidder's Single Largest Completed Contract (SLCC) similar to the contract to be bid

Business Name : ______________________
Business Address : ______________________

Name of Contract	a. Owner's Name b. Address c. Telephone Nos.	Nature of Work	Contractor's Role		a. Amount at Award b. Amount at Completion c. Duration	a. Date Awarded b. Contract Effectivity c. Date Completed
			Description	%		

Notes: 1. The bidder must state only one (1) Single Largest Completed Contract (SLCC) similar to the contract to be bid.
2. Supporting documents such as any of the following: Certificate of Acceptance; *or* Certificate of Completion; *or* Official Receipt (O.R); or Sales Invoice for the contract stated above shall be submitted during Bid Opening.

Submitted by : ______________________
(Printed Name & Signature)

Designation : ______________________
Date : ______________________

Standard Form Number: NPCSF-GOODS-04

NET FINANCIAL CONTRACTING CAPACITY (NFCC)

A. Summary of the Supplier's/Distributor's/Manufacturer's assets and liabilities on the basis of the income tax return and audited financial statement for the immediately preceding calendar year are:

		Year 20__
1.	Total Assets	
2.	Current Assets	
3.	Total Liabilities	
4.	Current Liabilities	
5.	Net Worth (1-3)	
6.	Net Working Capital (2-4)	

B. The Net Financial Contracting Capacity (NFCC) based on the above data is computed as follows:

NFCC = [(Current assets minus current liabilities) x 15] minus the value of all outstanding or uncompleted portions of the projects under ongoing contracts, including awarded contracts yet to be started coinciding with the contract for this Project.

NFCC = P ______________________________

Herewith attached is certified true copy of the audited financial statement, stamped "RECEIVED" by the BIR or BIR authorized collecting agent for the immediately preceding calendar year.

Submitted by:

____

Name of Supplier / Distributor / Manufacturer

____

Signature of Authorized Representative

Date : ______________________

Standard Form Number: NPCSF-GOODS-05

JOINT VENTURE AGREEMENT

KNOW ALL MEN BY THESE PRESENTS:

That this JOINT VENTURE AGREEMENT is entered into by and between: ____________________, of legal age, *(civil status)* ________, authorized representative of ____________________ and a resident of ____________________.

- and –

____________________, of legal age, *(civil status)* ________, authorized representative of ____________________ a resident of ______________________________.

That both parties agree to join together their capital, manpower, equipment, and other resources and efforts to enable the Joint Venture to participate in the Bidding and Undertaking of the hereunder stated Contract of the **National Power Corporation.**

NAME OF PROJECT	**CONTRACT AMOUNT**

That the capital contribution of each member firm:

NAME OF FIRM	CAPITAL CONTRIBUTION
1.	₱
2.	₱

That both parties agree to be jointly and severally liable for their participation in the Bidding and Undertaking of the said contract.

That both parties agree that ________________ and/or ________________ shall be the Official Representative/s of the Joint Venture, and are granted full power and authority to do, execute and perform any and all acts necessary and/or to represent the Joint Venture in the Bidding and Undertaking of the said contract, as fully and effectively and the Joint Venture may do and if personally present with full power of substitution and revocation.

That this Joint Venture Agreement shall remain in effect only for the above stated Contract until terminated by both parties.

____________________ *Name & Signature of Authorized Representative*	____________________ *Name & Signature of Authorized Representative*
____________________ *Official Designation*	____________________ *Official Designation*
____________________ *Name of Firm*	____________________ *Name of Firm*

Witnesses

1. ____________________ 2. ____________________

[Jurat]

[Format shall be based on the latest Rules on Notarial Practice]

Standard Form Number: NPCSF-GOODS-06a

FORM OF BID SECURITY (BANK GUARANTEE)

WHEREAS, *(Name of Bidder)* ____________ (hereinafter called "the Bidder") has submitted his bid dated *(Date)*____________ for the *[name of project]* (hereinafter called "the Bid").

KNOW ALL MEN by these presents that We *(Name of Bank)* ____________ of *(Name of Country)* ____________ having our registered office at ____________ (hereinafter called "the Bank" are bound unto National Power Corporation (hereinafter called "the Entity") in the sum of *[amount in words & figures as prescribed in the bidding documents]* for which payment well and truly to be made to the said Entity the Bank binds himself, his successors and assigns by these presents.

SEALED with the Common Seal of the said Bank this _____ day of _________ 20___.

THE CONDITIONS of this obligation are that:

1) if the Bidder withdraws his Bid during the period of bid validity specified in the Bidding Documents; or

2) if the Bidder does not accept the correction of arithmetical errors of his bid price in accordance with the Instructions to Bidder; or

3) if the Bidder, having determined as the LCB, fails or refuses to submit the required tax clearance, latest income and business tax returns and PhilGEPs registration certificate within the prescribed period; or

4) if the Bidder having been notified of the acceptance of his bid and award of contract to him by the Entity during the period of bid validity:

   a) fails or refuses to execute the Contract; or

   b) fails or refuses to submit the required valid JVA, if applicable; or

   c) fails or refuses to furnish the Performance Security in accordance with the Instructions to Bidders;

we undertake to pay to the Entity up to the above amount upon receipt of his first written demand, without the Entity having to substantiate its demand, provided that in his demand the Entity will note that the amount claimed by it is due to the occurrence of any one or combination of the four (4) conditions stated above.

The Guarantee will remain in force up to 120 days after the opening of bids or as it may be extended by the Entity, notice of which extension(s) to the Bank is hereby waived. Any demand in respect of this Guarantee should reach the Bank not later than the above date.

DATE ________ SIGNATURE OF THE BANK ____________________

WITNESS ______ SEAL ____________________________

____

(Signature, Name and Address)

Standard Form Number: NPCSF-GOODS-06b

FORM OF BID SECURITY (SURETY BOND)

BOND NO.: ____________________ DATE BOND EXECUTED: ________________

By this bond, We (*Name of Bidder*) ________ (hereinafter called "the Principal") and *(Name of Surety)* ________________ of (*Name of Country of Surety)* ______________, authorized to transact business in the Philippines (hereinafter called "the Surety") are held and firmly bound unto National Power Corporation (hereinafter called "the Employer") as Obligee, in the sum of *(amount in words & figures as prescribed in the bidding documents)*, callable on demand, for the payment of which sum, well and truly to be made, we, the said Principal and Surety bind ourselves, our successors and assigns, jointly and severally, firmly by these presents.

SEALED with our seals and dated this _____ day of ____________ 20 ________

WHEREAS, the Principal has submitted a written Bid to the Employer dated the ______ day of ____________ 20 ______, for the ____________________ (hereinafter called "the Bid").

NOW, THEREFORE, the conditions of this obligation are:

1) if the Bidder withdraws his Bid during the period of bid validity specified in the Bidding Documents; or

2) if the Bidder does not accept the correction of arithmetical errors of his bid price in accordance with the Instructions to Bidder; or

3) if the Bidder, having determined as the LCB, fails or refuses to submit the required tax clearance, latest income and business tax returns and PhilGEPs registration certificate within the prescribed period; or

4) if the Bidder having been notified of the acceptance of his bid and award of contract to him by the Entity during the period of bid validity:

   d) fails or refuses to execute the Contract; or

   e) fails or refuses to submit the required valid JVA, if applicable; or

   f) fails or refuses to furnish the Performance Security in accordance with the Instructions to Bidders;

then this obligation shall remain in full force and effect, otherwise it shall be null and void.

PROVIDED HOWEVER, that the Surety shall not be:

a) liable for a greater sum than the specified penalty of this bond, nor

b) liable for a greater sum that the difference between the amount of the said Principal's Bid and the amount of the Bid that is accepted by the Employer.

Standard Form Number: NPCSF-GOODS-06b
Page 2 of 2

This Surety executing this instrument hereby agrees that its obligation shall be valid for 120 calendar days after the deadline for submission of Bids as such deadline is stated in the Instructions to Bidders or as it may be extended by the Employer, notice of which extension(s) to the Surety is hereby waived.

PRINCIPAL ______________________ SURETY ______________________

SIGNATURE(S) ______________________ SIGNATURES(S) ______________________

NAME(S) AND TITLE(S) ______________ NAME(S) ______________________

SEAL ______________________ SEAL ______________________

Standard Form No: NPCSF-GOODS-06c

REPUBLIC OF THE PHILIPPINES)
CITY OF ________________________) S.S.

BID-SECURING DECLARATION
TWO (2) YEARS OF LICENSE AND TECHNICAL SUPPORT OF THE EXISTING ANTIVIRUS
(PR NO. HO-IST25-005)

To: **National Power Corporation**
Gabriel Y. Itchon Building
Sen. Miriam P. Defensor-Santiago Ave.
(formerly BIR Road) corner Quezon Avenue
Diliman, Quezon City, Philippines 1100

I/We[1], the undersigned, declare that:

1. *I/We* understand that, according to your conditions, bids must be supported by a Bid Security, which may be in the form of a Bid-Securing Declaration.
2. *I/We* accept that: (a) *I/we* will be automatically disqualified from bidding for any contract with any procuring entity for a period of two (2) years upon receipt of your Blacklisting Order; and, (b) *I/we* will pay the applicable fine provided under Section 6 of the Guidelines on the Use of Bid Securing Declaration, within fifteen (15) days from receipt of the written demand by the Procuring Entity for the commission of acts resulting to the enforcement of the Bid Securing Declaration under Sections 23.1 (b), 34.2, 40.1 and 69.1, except 69.1 (f) of the IRR of R.A. 9184; without prejudice to other legal action the government may undertake.
3. *I/We* understand that this Bid-Securing Declaration shall cease to be valid on the following circumstances:

   (a) Upon expiration of the bid validity period, or any extension thereof pursuant to your request;

   (b) *I am/we are* declared ineligible or post-disqualified upon receipt of your notice to such effect, and (i) *I/we* failed to timely file a request for reconsideration or (ii) *I/we* filed a waiver to avail of said right;

   (c) *I am/we are* declared as the bidder with the Lowest Calculated and Responsive Bid, and *I/we* have furnished the performance security and signed the Contract.

IN WITNESS WHEREOF, *I/we* have hereunto set my hand this ____ day of ____ 20____ at ___________, Philippines.

____
[Name and Signature of Bidder's Representative/ Authorized Signatory]
[Signatory's legal capacity]
Affiant

[Jurat]
[Format shall be based on the latest Rules on Notarial Practice]

[1] *Select one and delete the other. Adopt same instruction for similar terms throughout the document.*

Standard Form No: NPCSF-GOODS-07

Omnibus Sworn Statement (Revised)

REPUBLIC OF THE PHILIPPINES)
CITY/MUNICIPALITY OF ______) S.S.

AFFIDAVIT

I, [Name of Affiant], of legal age, [Civil Status], [Nationality], and residing at [Address of Affiant], after having been duly sworn in accordance with law, do hereby depose and state that:

1. *[Select one, delete the other:]*

   [If a sole proprietorship:] I am the sole proprietor or authorized representative of [Name of Bidder] with office address at [address of Bidder];

   [If a partnership, corporation, cooperative, or joint venture:] I am the duly authorized and designated representative of [Name of Bidder] with office address at [address of Bidder];

2. *[Select one, delete the other:]*

   [If a sole proprietorship:] As the owner and sole proprietor, or authorized representative of [Name of Bidder], I have full power and authority to do, execute and perform any and all acts necessary to participate, submit the bid, and to sign and execute the ensuing contract for [Name of the Project] of the [Name of the Procuring Entity], as shown in the attached duly notarized Special Power of Attorney;

   [If a partnership, corporation, cooperative, or joint venture:] I am granted full power and authority to do, execute and perform any and all acts necessary to participate, submit the bid, and to sign and execute the ensuing contract for [Name of the Project] of the [Name of the Procuring Entity], as shown in the attached [state title of attached document showing proof of authorization (e.g., duly notarized Secretary's Certificate, Board/Partnership Resolution, or Special Power of Attorney, whichever is applicable;)];

3. [Name of Bidder] is not "blacklisted" or barred from bidding by the Government of the Philippines or any of its agencies, offices, corporations, or Local Government Units, foreign government/foreign or international financing institution whose blacklisting rules have been recognized by the Government Procurement Policy Board, by itself or by relation, membership, association, affiliation, or controlling interest with another blacklisted person or entity as defined and provided for in the Uniform Guidelines on Blacklisting;

4. Each of the documents submitted in satisfaction of the bidding requirements is an authentic copy of the original, complete, and all statements and information provided therein are true and correct;

5. [Name of Bidder] is authorizing the Head of the Procuring Entity or its duly authorized representative(s) to verify all the documents submitted;

6. *[Select one, delete the rest:]*

   [If a sole proprietorship:] The owner or sole proprietor is not related to the Head of the Procuring Entity, members of the Bids and Awards Committee (BAC), the Technical Working Group, and the BAC Secretariat, the head of the Project Management Office or the end-user unit, and the project consultants by consanguinity or affinity up to the third civil degree;

   [If a partnership or cooperative:] None of the officers and members of *[Name of Bidder]* is related to the Head of the Procuring Entity, members of the Bids and Awards Committee

(BAC), the Technical Working Group, and the BAC Secretariat, the head of the Project Management Office or the end-user unit, and the project consultants by consanguinity or affinity up to the third civil degree;

[If a corporation or joint venture:] None of the officers, directors, and controlling stockholders of *[Name of Bidder]* is related to the Head of the Procuring Entity, members of the Bids and Awards Committee (BAC), the Technical Working Group, and the BAC Secretariat, the head of the Project Management Office or the end-user unit, and the project consultants by consanguinity or affinity up to the third civil degree;

7. *[Name of Bidder]* complies with existing labor laws and standards; and

8. *[Name of Bidder]* is aware of and has undertaken the responsibilities as a Bidder in compliance with the Philippine Bidding Documents, which includes:

   a. Carefully examining all of the Bidding Documents;

   b. Acknowledging all conditions, local or otherwise, affecting the implementation of the Contract;

   c. Making an estimate of the facilities available and needed for the contract to be bid, if any; and

   d. Inquiring or securing Supplemental/Bid Bulletin(s) issued for the *[Name of the Project]*.

9. *[Name of Bidder]* did not give or pay directly or indirectly, any commission, amount, fee, or any form of consideration, pecuniary or otherwise, to any person or official, personnel or representative of the government in relation to any procurement project or activity.

10. In case advance payment was made or given, failure to perform or deliver any of the obligations and undertakings in the contract shall be sufficient grounds to constitute criminal liability for Swindling (Estafa) or the commission of fraud with unfaithfulness or abuse of confidence through misappropriating or converting any payment received by a person or entity under an obligation involving the duty to deliver certain goods or services, to the prejudice of the public and the government of the Philippines pursuant to Article 315 of Act No. 3815 s. 1930, as amended, or the Revised Penal Code.

IN WITNESS WHEREOF, I have hereunto set my hand this __ day of ___, 20__ at __________, Philippines.

[Insert NAME OF BIDDER OR ITS AUTHORIZED REPRESENTATIVE]
[Insert signatory's legal capacity]
Affiant

[Jurat]
[Format shall be based on the latest Rules on Notarial Practice]

Standard Form No: NPCSF-GOODS-08

BID LETTER

Date: ______________

To: **THE PRESIDENT**
National Power Corporation
Gabriel Y. Itchon Building
Sen. Miriam P. Defensor-Santiago Ave.
(formerly BIR Road) corner Quezon Avenue
Diliman, Quezon City, Philippines 1100

Gentlemen:

Having examined the Bidding Documents including Bid Bulletin Numbers *[insert numbers]*____, the receipt of which is hereby duly acknowledged, we, the undersigned, offer to perform **TWO (2) YEARS OF LICENSE AND TECHNICAL SUPPORT OF THE EXISTING ANTIVIRUS (PR NO. HO-IST25-005)** in conformity with the said Bidding Documents for the sum of *[total Bid amount in words and figures]*______________________________ or such other sums as may be ascertained in accordance with the Schedule of Prices attached herewith and made part of this Bid.

We undertake, if our Bid is accepted, to supply and deliver the goods and perform other services, if required within the contract duration and in accordance with the scope of the contract specified in the Schedule of Requirements and Technical Specifications.

If our Bid is accepted, we undertake to provide a performance security in the form, amounts, and within the times specified in the Bidding Documents.

We agree to abide by this Bid for the Bid Validity Period specified in Bid Documents and it shall remain binding upon us and may be accepted at any time before the expiration of that period.

Until a formal Contract is prepared and executed, this Bid, together with your written acceptance thereof and your Notice of Award, shall be binding upon us.

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

We certify/confirm that we comply with the eligibility requirements pursuant to the Bidding Documents.

We likewise certify/confirm that the undersigned, ***[for sole proprietorships, insert:*** as the owner and sole proprietor or authorized representative of *[Name of Bidder]*__________________has the full power and authority to participate, submit the bid, and to sign and execute the ensuing contract, on the latter's behalf for the *[Name of Project]*______________ of the National Power Corporation ***[for partnerships, corporations, cooperatives, or joint ventures, insert:*** is granted full power and authority by the *[Name of Bidder]*______________________________ to participate, submit the bid, and to sign and execute the ensuing contract on the latter's behalf for *[Name of Project]*______________ of the National Power Corporation.

We acknowledge that failure to sign each and every page of this Bid Letter, including the attached Schedule of Requirements (Bid Price Schedule), shall be a ground for the rejection of our bid.

______________________________ ______________________________
[name and signature of authorized signatory] *[in the capacity of]*

Duly authorized to sign Bid for and on behalf of ______________________________
[name of bidder]

Bank Guarantee Form for Advance Payment

To: **THE PRESIDENT**
National Power Corportion
Gabriel Y. Itchon Building
Sen. Miriam P. Defensor-Santiago Ave.
(formerly BIR Road) corner Quezon Avenue
Diliman, Quezon City, Philippines 1100

[name of Contract]

Gentlemen and/or Ladies:

In accordance with the Advance Payment Provision, of the General Conditions of Contract, *[name and address of Supplier]* (hereinafter called the "Supplier") shall deposit with the PROCURING ENTITY a bank guarantee to guarantee its proper and faithful performance under the said Clause of the Contract in an amount of *[amount of guarantee in figures and words]*.

We, the *[name of the universal/commercial bank]*, as instructed by the Supplier, agree unconditionally and irrevocably to guarantee as primary obligator and not as surety merely, the payment to the PROCURING ENTITY on its first demand without whatsoever right of objection on our part and without its first claim to the Supplier, in the amount not exceeding *[amount of guarantee in figures and words]*.

We further agree that no change or addition to or other modification of the terms of the Contract to be performed thereunder or of any of the Contract documents which may be made between the PROCURING ENTITY and the Supplier, shall in any way release us from any liability under this guarantee, and we hereby waive notice of any such change, addition, or modification.

This guarantee shall remain valid and in full effect from the date the advance payment is received by the Supplier under the Contract and until the Goods are accepted by the PROCURING ENTITY.

Yours truly,

Signature and seal of the Guarantors

____
[name of bank or financial institution]

____
[address]

____
[date]

CERTIFICATION AS A DOMESTIC BIDDER

This is to certify that based on the records of this office, *(Name of Bidder)* ______________ is duly registered with the DTI on ______________.

This further certifies that the articles forming part of the product of *(Name of Bidder)* ______. which are/is *(Specify)* ______________________________ are substantially composed of articles, materials, or supplies grown, produced or manufactured in the Philippines. (Please encircle the applicable description/s).

This certification is issued upon the request of *(Name of Person/Entity)* ______________ in connection with his intention to participate in the bidding for the *(Name of Project)* ______________ of the National Power Corporation (NPC).

Given this __ day of ____________20__ at ____________, Philippines

____
Name

____
Position

____
Department of Trade & Industry