



Ceylon Petroleum Corporation

Anti-Virus Solution for CPC for three years period

B/ 49 /2020

BIDDING DOCUMENT

2020

TENDER NOTICE
CEYLON PETROLEUM CORPORATION
ANTI-VIRUS SOLUTION FOR CPC FOR THREE YEARS PERIOD
B/49 /2020

The Chairman, Procurement Committee, Ceylon Petroleum Corporation will receive National Competitive Bids from Manufacturers or their Accredited Local Agents for the Anti-Virus Solutions.

Bidding documents can be obtained between **0900 hrs. and 1500 hrs. up to 03.11.2020** from the office of Manager (Procurement & Stores), Ceylon Petroleum Corporation, 1st. Floor, No. 609, Dr. Danister De Silva Mwt., Colombo 09, on a written request and on payment of non-refundable fee of Rs. 1,000.00 (Rs. 925.63 + 8% VAT) per set.

The Bid will be closed at **1400 hrs. on 04.11.2020** and opened at the Office of Manager (Procurement & Stores), immediately after closing time of the Bid. Bidders or their authorized representatives will be permitted to be present at the opening of the Bid.

Bids may be sent by post under registered cover or may be deposited in the Tender Box kept in the Office of Manager (Procurement & Stores), Ceylon Petroleum Corporation, 01st Floor, No. 609, Dr. Danister De Silva Mwt, Colombo 09.

Bidding documents may be inspected upto **1500 hrs 03.11.2020** at the Office of Manager (Procurement & Stores), Ceylon Petroleum Corporation, 01st Floor, No, 609, Dr. Danister De Silva Mawatha, Colombo 09.

Clarifications (if any) shall be sought from the under mentioned Telephone/Fax numbers.

<p>Due to the Covid-19 pandemic, the bidders can download the bidding document from CPC website, i.e - www.ceypetco.gov.lk , and all the payment can be made to the Account No. 00410011020 of Ceylon Petroleum Corporation of People's Bank (Head Office)</p>

Chairman,
Departmental Procurement Committee,
c/o Manager (Procurement & Stores),
Ceylon Petroleum Corporation,
No. 609, Dr. Danister De Silva Mawatha,
Colombo 09,
Sri Lanka.
Tele : 0094-11-5455330, 5455337
Fax : 0094-11-5455424

Table of Contents

1. INSTRUCTIONS TO BIDDERS	5
1.1 Introduction	5
1.2 Content of the Bidding Documents	5
1.3 Eligibility Requirement	5
1.4 Scope or Work	6
1.5 Documents to accompany the Bid	7
1.6 Sealing and marking of Bids	8
1.7 Period of validity of Bids	8
1.8 Signing of Bids	8
1.9 Clarification of Bidding Document	9
1.10 Deadline for submission of Bids	9
1.11 Late Bids	9
1.12 Withdrawal of Bids	9
1.13 Closing of Bids	9
1.14 Opening of Bids by CPC	9
1.15 Agent's Authority:	10
1.16 Bid Security Guarantee	10
1.17 Schedule of Prices	10
1.18 Preliminary Examination of Bids	10
1.19 Correction of Errors	11
1.20 Evaluation of Bids:	11
1.21 CPC's right to accept or reject any or all Bids	11
1.22 Notice of Acceptance	11
1.23 Award Criteria	12
2. CONDITIONS OF CONTRACT (COC)	13
2.1 Performance Security:	13
2.2 Warranty Conditions	13

2.3	Delivery Period	13
2.4	Defaults by Successful Bidder	13
2.5	Liquidated Damages	14
2.6	Force Majeure:	14
2.7	Arbitration	14
2.8	Termination	14
2.9	Governing Law	14
3.	TECHNICAL SPECIFICATIONS.	15
	Technical Specifications for Anti-Virus Client Software (Desktops & Servers)	15
	Technical Specifications for Upgrading of Existing Antivirus Server Hardware & Software	25
4.	BILL OF QUANTITIES	26
	ANNEX-A : Form of Bid	27
	ANNEXURE - B - Format for Bid Security Guarantee	29
	ANNEXURE - C : Form of Agreement	31
	ANNEXURE - D - Format for Performance Guarantee	33

1. INSTRUCTIONS TO BIDDERS

1.1 Introduction

- 1.1.1. Ceylon Petroleum Corporation (CPC) is calling Bids from internationally reputed Manufacturers or their Local Agents/ Sole Distributors in Sri Lanka for Anti-Virus Solution for CPC for CPC for three years period on the basis of ex-stock or delivered in Colombo.

1.2 Content of the Bidding Documents

- 1.2.1 Bidding Document will consist of the followings ;
- 1.2.1.1 Instructions to Bidders (ITB)
 - 1.2.1.2 Conditions of Contract (COC)
 - 1.2.1.3 Particular Conditions of Contract
 - 1.2.1.4 Technical Specifications
 - 1.2.1.5 Schedule of Prices
 - 1.2.1.6 Form of Bid

1.3 Eligibility Requirement

- 1.3.1 The quoted antivirus solution manufacturer should be ISO/IEC 27001:2013 (for information security management system) accredited and documentary evidence should be included. **If the bidder has not submitted proof documents CPC will treat the offer as non-responsive.**
- 1.3.2 The bidder should be ISO 9001:2015 accredited and documentary evidence should be included.
- 1.3.3 The bidder shall have proven experience for supplying Network Security Solutions
(Proof documents shall be attached with the proposal). **If the bidder has not submitted proof document CPC will treat the offer as non-responsive.**
- 1.3.4 The bidder or its subsidiaries or affiliated companies should not be blacklisted by any government institution during the past 10 years. Bidder should submit the Letter.
- 1.3.5 The bidder shall have been in the business as of the nature of the goods and service of this contract for at least 05 years from the date of the registration. **Documentary evidence shall be produced to this.**

- 1.3.6 Bidder should submit a manufacturer authorization letter from the antivirus solution manufacturer. If the manufacture authorization letter is not submitted with the bid submission, CPC will treat the bid as a nonresponsive offer.
- 1.3.7 The bidder should have trained engineering resources for the quoted Antivirus Solution, documentary evidence should be provided
- 1.3.8 The quoted product should have at least 3 implementations of similar complexity in the Sri Lanka and should have been completed during the last 5-years, documentary evidence should be provided.
- 1.3.9 The Bidder should agree to locate (In head office Premises) to Technical person to during the entire installation period.
- 1.3.10 Detail system implementation project plan should be provided with the bid submission.

1.4 Scope or Work

- 1.4.1 Assessing the existing network infrastructure and planning for an optimal deployment strategy for CPC head office and island wide branch locations (20 island wide branches).

	Location	Primary Link Bandwidth	No.Desktops
1	Head Office - Colombo -09	6mbps	450
2	Refinery - Sapugaskanda	2mbps	100
3	Aviation - Katunayake	512kbps	25
4	New Terminal - Sapugaskanda	512kbps	20
5	Area Office Nugegoda	256kbps	20
6	Aviation - Kurunegala	256kbps	13
7	Area Office Anuradhapura	256kbps	13
8	Area Office Peradeniya	256kbps	13
9	Area Office Kegalle	256kbps	12
10	Aviation - Mattala	512kbps	11
11	Area Office Galle	256kbps	10
12	Area Office Batticaloa	256kbps	10
13	Area Office Jaffna	256kbps	9
14	Area Office Badulla	256kbps	8
15	Sales Center Muthurajawela	256kbps	7
16	SSE Workshop	256kbps	7
17	Aviation - Rathmalana	128kbps	3
17	Agro Kandy	128kbps	2

18	Agro Nuwara Eliya	128kbps	1
19	Agro Anuradhapura	128kbps	1
20	Agro Kolonnawa*		13
	Total		748
1	E Banking System	Servers	6
2	Domain	Servers	2
3	Data Base	Servers	2
	Total	Servers	10

- 1.4.2 Installation of the antivirus system management application framework with all related software components. Existing hardware platforms where possible should be best utilized for the system deployment.
- 1.4.3 Creation of the client installation packages taking into consideration the bandwidth limitations of the wide area network.
- 1.4.4 Complete deployment of the antivirus solution at CPC head office and Island wide branch network with minimum impact to the business process.
- 1.4.5 Providing administrator level hands on training for nominated CPC IT staff members at CPC head office and Refinery.
- 1.4.6 Preparation and hand over of as build documentation related to client agent deployment and management console usage for day to day system administration work.
- 1.4.7 Setting up of a remote monitoring console and emergency alert notification platform, in order to take necessary precautionary actions should there be a malware or a virus attack.
- 1.4.8 Deploying a redundant antivirus management server and configuring the clients to access and receive updates in an event if the primary server is unavailable.

1.5 Documents to accompany the Bid

- 1.5.1 All Bidders shall furnish adequate information in respect of the items offered.
- 1.5.2 Failure to furnish the following documents and details, with the bid may result in the Bid being rejected. All documents shall be furnished in English language.
 - 1.5.2.1 Experience of the vender
 - 1.5.2.2 Past performance – Bidders should forward past supply records for the last Three (03) years.
 - 1.5.2.3 Manufacturers certified authorization to quote
 - 1.5.2.4 Business Registration Certificate of the Company.

- 1.5.2.5 Brand Name and the Country of Manufacturer of the items offered.
- 1.5.2.6 Certificate from the manufacturer to certify that the items offered are of currently in manufacture.
- 1.5.2.7 Every Bidder should specify the conditions and period of warranty.
- 1.5.2.8 Detailed Technical Specifications and literature of the item offered.
- 1.5.2.9 Schedule of Prices duly completed and signed.
- 1.5.2.10 Form of Bid (Annex A) duly completed and signed.

1.6 Sealing and marking of Bids

- 1.6.1 Bids shall be submitted in duplicates. The original and the duplicate of the Bid shall be placed in separate envelopes marked 'ORIGINAL' and 'DUPLICATE' and shall be marked "ANTI-VIRUS SOLUTION FOR CPC FOR THREE YEARS PERIOD" (The Invitation to Bid title) on the top left hand corner and the statement, "DO NOT OPEN BEFORE **1400 hrs on 04.11.2020** (to be completed with the time and date specified in the Bidding Document.

Manager (Procurement & Stores),
Procurement & Stores Function,
1st Floor, No. 609,
Dr. Danister De Silva Mawatha,
Colombo 09.
Sri Lanka.

- 1.6.2 If the envelope is not sealed and marked as stated above, CPC will not take the responsibility for the Bids being misplaced or premature opening. In the event of any discrepancy between the Original and the Duplicate, the Original shall govern.

1.7 Period of validity of Bids

- 1.7.1 All bids shall be valid for a minimum period of Seventy Seven (77) days from the closing date of the Bid. A Bid valid for a shorter period will be rejected as non-responsive.

1.8 Signing of Bids

- 1.8.1 The Original and the Duplicate of the Bid shall be typed, or written in indelible ink, and shall be signed by the Bidder. All pages of the Bid except for un-amended printed literature shall be initialed by the person(s) signing the Bid.
- 1.8.2 Any inter lineation, erasures or over-writing shall be valid only if they are initialed by the person(s) signing the Bid.

1.9 Clarification of Bidding Document

- 1.9.1 A prospective Bidder requiring any clarification of the Bidding Document should notify CPC in writing by hand or post or facsimile at the CPC's mailing address indicated in the Bidding Document clause 1.4. Similarly if a Bidder feels that any important provision is unacceptable, such objection should be raised at this stage. CPC will respond in writing to any request for clarification or modification of the Bidding Document that is received not later than Seven (07) days prior to the deadline of submission of Bids prescribed by the CPC.

1.10 Deadline for submission of Bids

- 1.10.1 CPC must receive Bids at the address specified in ITB Clause 1.4, not later than 1400 hrs. on 04.11.2020.

1.11 Late Bids

- 1.11.1 Any Bid received by CPC after the deadline for submission of Bids, will be rejected and returned unopened to the Bidder.

1.12 Withdrawal of Bids

- 1.12.1 A Bidder wishing to withdraw his Bid shall notify the CPC in writing prior to the deadline prescribed for the submission of Bids. A withdrawal notice may also be sent by Facsimile, but must be followed by the original, by post or by hand not later than the deadline for submission of Bids. The notice of withdrawal shall be sent to the Manager (Procurement & Stores), which the address is given in Clause No. 1.4.

1.13 Closing of Bids

- 1.13.1 Bids shall be closed at 1400 hrs on 04.11.2020 and hence bids shall be reached to the address given in clause no. 1.4 before the time and date specified in clause no. 1.8.

1.14 Opening of Bids by CPC

- 1.14.1 Bids will be opened immediately after the closing date and time fixed for receipt of Bids. The address where bids are opened is given in clause 1.4.

1.15 Agent's Authority:

- 1.15.1 An Accredited Agent of the manufacture signing the Bidding Document on behalf of the Principal shall state the Principal's name and address, telephone number and fax number, (if any) and a letter of Authority empowering the agent.
- 1.15.2 Nomination of an Agent after the Bid has been submitted will not be valid.

1.16 Bid Security Guarantee

- 1.16.1 Each Bid shall be accompanied by a Bid Security Guarantee, (if requested) undertaking that the bid will be held valid for the specified period, and that the bid will not be withdrawn during that period. Such security shall be in the form of a Bank Draft or a Bank Guarantee issued / confirmed by a recognized Bank in Sri Lanka, and payable to the CPC on demand in a sum of Rupees Seventy Five Thousand Only (Rs. 75,000.00).
- 1.16.2 The Bid Security Guarantee should be valid for hundred and Seven (107) days (i.e. 18.02.2021) from the date of closing of Bid. A form of Bid Security Guarantee is attached in Annex "B".
- 1.16.3 Failure to submit the Bid Security Guarantee at the time, or before the closing of Bid, and in accordance with above said requirements, and in the format provided, will result in the Bid being rejected. Bid Security Guarantee from unsuccessful Bidders will be returned to them after the award is made to the successful Bidder. The Bid Security of the successful Bidder will be returned only after receipt of the Performance Security Guarantee.

1.17 Schedule of Prices

- 1.17.1 Bidders are required to duly sign and return the "Schedule of Prices" as indicated in the bidding document.

1.18 Preliminary Examination of Bids

- 1.18.1 CPC will examine the Bids to determine whether they are complete, any computational errors have been made, whether the documents have been properly signed, and the Bids are generally in order. If not, CPC may at its discretion call clarifications from the Bidder. The request for clarification and the response shall be in writing within one week's form the clarifications and no change in the price or substance of the Bid shall be sought, offered or permitted.

1.19 Correction of Errors

- 1.19.1 Bids determined to be substantially responsive will be checked by the Employer for any arithmetic errors. Errors will be corrected by the Employer as follows:
- 1.19.1.1 Where there is a discrepancy between the amounts in figures and in words, the amount in words will govern; and
 - 1.19.1.2 Where there is a discrepancy between the unit rate and the line item total resulting from multiplying the unit rate by the quantity, the unit rate as quoted will govern, unless there is an obviously gross misplacement of the decimal point in the unit rate, in which case the line item total as quoted will govern, and the unit rate will be corrected.
 - 1.19.1.3 If the total Bid price increases due to corrections made on above procedure, the bid price shall not be adjusted to the increased price and the corrections should be readjusted within the Bid price in consultation with the Bidder.
 - 1.19.1.4 If the bid price decreases by the above procedure, the amount stated in the Form of Bid shall be adjusted with the concurrence of the Bidder and shall be considered as binding upon the Bidder.
 - 1.19.1.5 If the bidder does not accept the corrected amount of bid, its bid shall be rejected and the bid security may be forfeited.

1.20 Evaluation of Bids:

- 1.20.1 CPC will carry out a detailed evaluation of Bids, to determine whether the Technical aspects are properly addressed, and the Bids are substantially responsive.

1.21 CPC's right to accept or reject any or all Bids

- 1.21.1 The CPC will not be bound to make the award to the Bidder submitting the lowest offer.
- 1.21.2 The CPC reserves the right to reject any or all Bids or any part thereof, without assigning any reasons. The CPC may accept any or all items of an bid, and reserves the right to increase or decrease the number of units to be contracted for, at prices indicated in the Schedule of Prices.

1.22 Notice of Acceptance

- 1.22.1 The notice of acceptance of Bid will be sent by facsimile, followed by post to the successful Bidder, to the address given by him in the Bidding Document, soon after the decision of the CPC.

1.23 Award Criteria

- 1.23.1 Subject to ITB Clause 1. 18, the CPC will award the contract to the successful Bidder, whose Bid has been determined to be substantially responsive, lowest evaluated Bid, provided that the Bidder is determined to be qualified to perform the contract satisfactorily.
- 1.23.2 The successful Bidder will be called upon to supply or part there off conforming to Technical Specifications, and strictly by the agreed delivery date which should be within one month as per clause 2.4 of COC.
- 1.23.3 If The Successful bidder is called upon to enter in to and Agreement with CPC, the bidder should be ready to sign an agreement with CPC.

2. CONDITIONS OF CONTRACT (COC)

2.1 Performance Security:

- 2.1.1 If it is applicable, the successful Bidder will be notified by CPC to furnish a Performance Guarantee. This guarantee shall be submitted on his owned cost and within fourteen (14) days of such notification through / confirmed by a reputed Commercial Bank in operation in Sri Lanka, for a sum equivalent to 10% of the total Bid value of the accepted Bid. The Performance Security shall be complied to the format given in Annex D. The period of validity of this performance security shall be the expected period of delivery of goods/equipment plus one month.
- 2.1.2 If the successful Bidder fails to furnish the Performance Security aforesaid, his name will be placed in the list of defaulting Contractors. CPC shall therefore, be entitled in its absolute discretion to make suitable arrangements required for the performance of such Bid, as the case may be, at the risk and expense of the successful Bidder.
- 2.1.3 The successful Bidder, in the event of his failure to furnish the Performance Security as required, shall be liable for any losses, costs expenses and damages, which the CPC may sustain in consequence of such failure, and the Bid security shall be forfeited.

2.2 Warranty Conditions

- 2.2.1 The successful Bidder should give a Comprehensive Warranty from the Manufacturer for a period of one year from the date of delivery.

2.3 Delivery Period

- 2.3.1 Period of delivery shall be 30 days from the date of confirmation of the order.

2.4 Defaults by Successful Bidder

- 2.4.1 If the successful Bidder, defaults in the supply or otherwise commit a breach of any of the provisions in the Contract with CPC, he shall be liable to pay to CPC, all losses, damages and expenses incurred by CPC, in consequence of such default or breach. Bidders should declare that they had read the Bid conditions, and that they make the offer in compliance with, and subject to all the conditions

thereof, and agree to perform the services in accordance with the said conditions in the manner therein set out, and in terms of this offer. A Form of Bid, as Annex- 'A' is attached.

2.5 Liquidated Damages

2.5.1 Liquidated Damages amounts to Rs. 2,000.00 will be levied per each day delayed beyond the period of delivery specified in the contract.

2.6 Force Majeure:

2.6.1 Except as regards an act of God, War, Strike, Invasion, Civil war, Rebellion Revolution, Insurrection, Earthquake or Plagues, the Bidder shall undertake all risks and liabilities of whatsoever kind arising out of incidentals connected with the sale.

2.7 Arbitration

2.7.1 If during the continuance of this Contract or at any time after the termination thereof, any disputes or differences of opinion touching the interpretation of this contract were to arise between the parties hereto or their respective representatives, such differences or disputes shall be referred for Arbitration.

2.7.2 Arbitration shall be conducted under the rules of ICLP (Institute of the Development of Commercial Law & Practice), Arbitration Centre and in accordance with the arbitration Act No. 11 of 1995 of Sri Lanka. The place of Arbitration shall be Colombo, Sri Lanka.

2.8 Termination

2.8.1 Ceylon Petroleum Corporation may at any time terminate the contract by giving written notice to the supplier, if the Supplier breach of any of the provisions in the contract with CPC for the supply of vehicle/s or becomes bankrupt or otherwise insolvent. In this event, termination will be done without compensation to the Supplier, provided that such termination will not prejudice or effect any right of action or remedy which has accrued or will accrue thereafter to CPC.

2.9 Governing Law

2.9.1 The law of the Democratic Socialist Republic of Sri Lanka is applicable

3. TECHNICAL SPECIFICATIONS.

Technical Specifications for Anti-Virus Client Software (Desktops & Servers)

Compliance or non-compliance of all items to be specified in the relevant columns. In all cases accurate cross reference to technical literature by indicating the folio number etc. to be mentioned. Sufficient and authentic technical literatures to support claims of compliance to be provided. Bidder’s failure to provide the information requested in the relevant columns may be a reason for the rejection of the bid.

Minimum Technical Specifications		Bidder Response (Yes/No)	Detail Response
1.	Make		
2.	Model		
3.	Country of Origin		
4.	Country of Manufacture		
5.	Manufacture Authorization		
6.	3 Year Comprehensive security updates and hot fixes for security threats		
7.	Should include the quantity of licenses mention in BOQ (Desktop / Server client licenses) and all associated components for centralized management should be provided.		
8.	Bidder should provide necessary training and documentation for nominated CPC staff to maintain the system.		
9.	All related configuration documentation should be provided by the bidder.		
Operating system compatibility			
10.	Should support desktop operating systems	<ul style="list-style-type: none"> • Windows 10 • Windows 8.1 • Windows 8 • Windows 7 	

11	Should support Operating system virtual patching for	<ul style="list-style-type: none"> • Windows 10 • Windows 8.1 • Windows 8 • Windows 7 		
12	Multi-Platform Management Windows, Mac and Linux machines must be managed from one management console.			
13	Updating Bandwidth Consumption <ul style="list-style-type: none"> • Updating of endpoints should have the ability to set pre-configured available bandwidth used for both software updating and threat definition updates (Ex: 64, 128, 256Kbps etc.) • Must have the option to setup local cache updating server within on-premise network environment to minimize large software engine update. • Must be able to add an Update Management Policy to allow setting of schedules for updating on the endpoint. 			
14	Deployment Options Deploying of the endpoint agent must support the following methodology:	<ul style="list-style-type: none"> • Email • Via AD Startup/Shutdown script • AD Login script • SCCM • Able to also include the installation to clone image 		
15	SIEM (Security information and event management) Integration Must have the capability to extract events and alerts information from the Cloud Dashboard to local SIEM integrating.			
16	Role Base Management (RBAC) Must have the capability to allow the separation of estate management to different administrator login.			
17	Microsoft AD Synchronization Must have the capability to only allow outbound synchronization of Users/Groups from the local Active Directory servers to the Cloud Dashboard for policy management.			
18	Policies Selected policies should be able to be applied to either users or devices.			

		Policies must be able to be disabled automatically based on a scheduled time and date		
19.	<p>Enhanced Tamper Protection</p> <p>The endpoint solution must have the capability to monitor or stop local administrative users or malicious processes to disable the endpoint protection:</p>	<ul style="list-style-type: none"> • Stopping services from the Services UI • Kill services from the Task Manager UI • Change Service Configuration from the Services UI • Stop Services / edit service configuration from the command line • Uninstall • Reinstall • Kill processes from the Task Manager UI • Delete or modify protected files or folders • Delete or modify protected registry keys 		
20.	<p>Advanced Deep Learning mechanism</p> <p>The system shall be light speed scanning, and the model shall be able to extract millions of features from a file, conduct a deep analysis, and determine if a file is benign or malicious. This entire process happens before the file executes.</p>	<ul style="list-style-type: none"> • 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 with offline and will not rely on signatures. • Must classify files as malicious, potentially unwanted apps (PUA) or benign. Deep learning must also focus on Windows portable executable. • Able to perform new Zero days threat scanning offline (without internet) • Must be Smarter - should be able to process data through multiple analysis layers, each layer making the model considerably more powerful. 		

		<ul style="list-style-type: none"> • Must be scalable - should be able to process significantly more input, can accurately predict threats while continuing to stay up to date. • Must Lighter - model footprint shall be incredibly small, less than 20MB on the endpoint, with almost zero impact on performance. • The Machine learning model shall be train and evaluate models end-to-end using advanced developed packages like Keras, Tensorflow, and Scikit-learn. 		
21	<p style="text-align: center;">Exploit Prevention / Mitigation on the known exploits</p>	<ul style="list-style-type: none"> • Enforcement of Data Execution Protection (DEP), Prevents abuse of buffer overflows • 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, Pre-allocated common memory areas to block example attacks • Dynamic Heap Spray, stops attacks that spray suspicious sequences on the heap • Stack Pivot, Stops abuse of the stack pointer • Stack Exec (MemProt), Stops attacker' code on the stack • Stack-based ROP Mitigations (Caller), Stops standard Return-Oriented Programming attacks 		

		<ul style="list-style-type: none"> • Branch-based ROP Mitigations (Hardware Augmented), Stops advanced Return-Oriented Programming attacks • Structured Exception Handler Overwrite Protection (SEHOP), Stops abuse of the exception handler • Import Address Table Access Filtering (IAF) (Hardware Augmented) Stops attackers that lookup API addresses in the IAT • Load Library API calls, Prevents 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 shell code involves multiple techniques to address things like fragmented shell code, encrypted payloads, and null free encoding. • VBScript God Mode, have the ability to detect the manipulating of the safe mode flag on VBScript in the web browser • WoW64, must have the ability to prohibits the program code from directly switching from 32-bit to 64-bit mode (e.g. using ROP), while still enabling the WoW64 layer to perform this transition. • Syscall, stops attackers that attempt to bypass security 		
--	--	--	--	--

		<p>hooks</p> <ul style="list-style-type: none"> • 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 		
22	<p>Malicious Traffic Detection (MTD)</p> <p>Must be able to detect communications between endpoint computers and command and control servers involved in botnet or other malware attacks.</p>			
23	<p>Anti-Ransomware Protection</p> <ul style="list-style-type: none"> • Must have the ability for the encrypted files to be rolled back to a pre-encrypted state. • Both Anti-Exploit and Ransomware protection do not need to have a Cloud Lookup to perform the detection. • When Anti-crypto function suspects that a certain behavior is not in keeping with its intended process, the Data Recorder 			

	<p>starts caching data while 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 200MB and the min individual file size that it would record is 25MB.</p> <ul style="list-style-type: none"> • The anti-crypto function shall look back at all the malicious file modifications made by that process and restores them to their original location. • Should a ransomware infection managed to get in, a detailed historical tracking of where the infection originated and how it propagated will be reported courtesy of the Threat Cases (RCA). 		
24	<p>Threat Cases</p> <ul style="list-style-type: none"> • Must have the capability to identify what happened, where a breach originated, what files were impacted, and provides guidance on how to strengthen an organization’s security posture • After an infection occurs Threat Cases (RCA) tracks data 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 halting the infection. • Threat Case shall provide summary of the event: What exploit was discovered. Where the beacon event occurred (an asset). When it occurred. How the infection succeeded. Ex: “Outlook.exe”. • Threat Cases shall provide recommendations to address the problem: Things to look for post-attack. Eg. Aside from files being restored from encrypted ones, check browser settings to ensure no vulnerabilities were created as result of the infections. • 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, and Closed) and to set priority (Low, Medium and High). When closing the administrator can add notes and is also required to confirm (via check boxes) that remediation steps were taken analyzed impact on files/assets and relevant environmental improvements were implemented. • Provides a tabular view of everything affected during the attack. Items can be filtered based on type. eg. Files, 		

	<p>processes, registry keys. The administrator can view information about each item eg. Filename (victim file or malware agent), process ID, start/stop timestamp of the event.</p> <ul style="list-style-type: none"> • Threat Cases shall clearly indicated the beginning of the root caused, 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 		
25	<p>Advance System Clean</p> <p>Must have the capability to trigger a deep clean upon any active detection from exploit or ransomware detection. The next gen endpoint shall provide advanced Clean detects malware by looking for the following:</p>	<p>Files :</p> <p>1 or more has been flagged as bad by Surfright Cloud File is a device driver. File has been downloaded from the internet Authors name / version information is missing from file properties Impersonating a common windows system file Reboot survivability is vigorously protected. Un-common file extension used Contains PE structure anomalies and suggestions of obfuscation</p> <p>Processes :</p> <p>Listening for incoming connections Missing source executable file No UI elements Address Space Layout Randomization (ASLR) has been removed from the system</p>	
26	<p>Must have the following protection features:</p> <p>A) Web Control capability to filter web traffic by Category,</p> <p>B) Application Control detection and blocking capability,</p>		

	<p>C)Peripheral Control detection/blocking capability</p> <p>D) Detect malicious network traffic to Command and Control servers</p> <ul style="list-style-type: none"> • Must have technology in the Server Protection agent that only allows approved applications to run on servers to controlling what can run and modify application. • Must be able to create trust between applications, controlling which application can update an application, and also provides a data feed on trusted applications which automatically configures the product based on which applications the server has installed. • Must be able to easily see which attributes and code segments are similar to “known-good” and “known bad” files so they can determine if a file should be blocked or allowed. • Must have intelligent Use Case - security teams must have the visibility and expertise they need to answer the tough questions that are asked as part of an incident response effort. • Must have a guided investigation - allows administrators to answer the tough questions about security incidents by providing visibility into the scope of an attack, how it started, what was impacted, and how to respond. • Must be able to respond to incident with a single click Security teams must have the visibility and expertise they need to answer questions that are part of incident response. • Following points must be easily traced: <ul style="list-style-type: none"> - Understand the scope and impact of security incidents - Detect attacks that may have gone unnoticed - Search for indicators of compromise across the network - Prioritize events for further investigation - Analyze files to determine if they are a threat or potentially unwanted - Confidently report on your organization’s security posture at any given moment" 		
27	<p>General Requirements</p> <ul style="list-style-type: none"> • The proposed product should have local references and experiences for similar deployments • The proposed solution should be in the leader’s quadrant of the latest Gartner’s report for EPP 		

	<ul style="list-style-type: none"> • The proposed solution should be in the leaders/recommended section in the latest Forrester Wave report for EPP • Bidder should provide all necessary infrastructure services and other accessories including hardware/ software and licenses • Bidder should provide 3 years warranty along with 24x7 support on all hardware/ software and other accessories and licenses • The bidder should be a well-established company which should have more than 5 years of operational history in the service integration segment • Vendor's JNCIE, CCIE, MVP, CISSP or equivalent certifications will take precedence during the technical evaluation • The bidder should provide 10 or more references of similar deployments of Endpoint Protection Platform 		
--	---	--	--

Technical Specifications for Upgrading of Existing Antivirus Server Hardware & Software

Minimum Technical Specifications		Bidder Response (Yes/No)	Detail Response
	The existing Dell R440 server bearing service Tag 275W8T2 must be upgraded to the below configuration or higher		
Operating System			
	Should be provided with Windows 2016 or latest with 5 client access licenses in each. All product activation keys should be licensed to Ceylon Petroleum Corporation (CPC).		
	Should include a commercial grade virtualization system compatible with the antivirus management system with a 3-year support and subscription plan. All product activation keys should be licensed to CPC.		
Installation and Configuration			
	The bidder should carry out turnkey system installation as per the industrial best practices for installing a virtualized server platform while segregating the system boot with the production data storage sub systems.		
	Any BIOS or system firmware upgrade should be carried out as per the server manufacturer's recommendations		
Original Equipment Vendor Support Services			
	All defective parts should be replaced free of charge with the brand-new parts during the warranty period from manufacture's authorized technical center.		
System Documentation			
	Complete system documentation related to the Server and the virtualization platform configuration together with the related resource allocation should be provided during the system handover.		
Server Hardware Warranty			
	3 Year on site comprehensive warranty and 5-year post warranty from the data of handing over of the antivirus system implementation. And 24x7 Services with Guaranteed SLA of 1 hour On Site Presence for All service-related issues.		
Bill of Material			
	Complete bill of materiel with all relevant part numbers should be provided together with the bid submission		

4. BILL OF QUANTITIES

Description		Qty.	Unit Price	Tax	Total Price
1	Antivirus, malware and end point protection system for desktops and laptops	750			
2	Antivirus, malware and threat protection systems for production servers	10			
3	Antivirus management / hosting server upgrade with windows 2016 or latest server licenses and industry standard virtualization platform with 3-years subscription and support plan (<i>Section 4.0 Dell R 440 Tag: 275W8T2</i>)	01			
Total (LKR)					

ANNEX-A : Form of Bid

To: The Chairman
Procurement Committee,
Ceylon Petroleum Corporation,
1st Floor,
No. 609, Dr. Danister De Silva Mawatha,.
Colombo 09.
SRI LANKA.

From:

.....

.....

Sir,

A-1 Having familiarized ourselves with the formal request for Instruction to Bidders and Conditions of contract, Technical Specification for Purchase of Anti-Virus Solution for CPC for three years period. We offer to complete the whole of said accessories in conformity with the said document.

A-2 Unless and until a formal agreement is prepared and executed this Bid together with your written acceptance thereof shall constitute a binding contract with us.

A-3 We understand you are not bound to accept the lowest or any Bid you may receive.

A-4 The Bid we are offering is complete and fulfils the requirements discussed in the Technical specifications of the Bidding Document.

A-5 We agree to abide by this Bid for the period of **Seventy Seven (77) days** from the date of opening of the same Bid. Conditions and prices quoted shall remain binding upon us and may be accepted at any time before the expiration of the period.

A-6 We agree to be bound by the Bid, Bid Conditions, Technical specifications and Performance security.

A-7 We affirm that the said items will be delivered within one month after we receive notice of acceptance of our Bid from the CPC.

A-8 We offer the lump sum fixed price of (foreign cost in figures)inwords)..... and Sri Lanka Rupees (local cost in figures) (in words..... for Supply of as detailed out in this Bidding Document and details of the lump sum price is as given in the schedule of prices. We agree that it is open to the Procurement Committee to reject this offer or to accept.

Dated this day of2020.
Signature.....in the capacity of
.....duly authorized to sign Bids for and on behalf of :

Name

Address
.....
.....

Witnesses:

- | | |
|--------------------|----------------------|
| 1. Signature | 2. Signature : |
| Name : | Name : |
| Address : | Address : |
| | |
| | |

ANNEXURE – B - Format for Bid Security Guarantee

[This Bank Guarantee form shall be filled in accordance with the instructions indicated in brackets]

.....[insert issuing agency’s name and address of issuing branch or office].....

Beneficiary : [insert (by PE) name and address of Employer/ Purchaser]

Date : [insert (by issuing agency) date]

BID GUARANTEE NO.:[insert (by issuing agency) number]

We have been informed that[insert (by issuing agency) name of the Bidder; if a joint venture, list complete legal names of partners] (hereinafter called “ the Bidder”) has submitted to you its bid dated[insert (by issuing agency) date] (hereinafter called “the Bid”) for execution/ supply [select appropriately] of [insert name of Contract] under Invitation for Bids No. [insert IFB number] (“the IFB”)

Furthermore, we understand that, according to your conditions, Bids must be supported by a Bid Guarantee.

At the request of the Bidder, we[insert name of issuing agency] hereby irrevocably undertake to pay you any sum or sums not exceeding in total an amount of[insert amount in figures][insert amount in words] upon receipt by us of your first demand in writing accompanied by a written statement stating that the Bidder is in breach of its obligation(s) under the bid conditions, because the Bidder.

- (a) has withdrawn its Bid during the period of bid validity specified; or
- (b) does not accept the correction of errors in accordance with the Instructions to Bidders (hereinafter “the ITB”) of the IFB; or
- (c) having been notified of the acceptance of its Bid by the Employer/ Purchaser during the period of bid validity, (i) fails or refuses to execute the Contract Form, if required, or (ii) fails or refuses to furnish the Performance Guarantee, in accordance with the ITB.

This Guarantee shall expire: (a) if the Bidder is the successful bidder, upon our receipt of copies of the Contract signed by the Bidder and of the Performance Guarantee issued to you by the Bidder; or (b) if the Bidder is not the successful bidder, upon the earlier of (i) our receipt of a copy of your notification to the Bidder that the Bidder was unsuccessful, otherwise it will remain in force up to[insert date]

Consequently, any demand for payment under this Guarantee must be received by us at the office on or before that date

[signature(s) of authorized representative(s)]

ANNEXURE - C : Form of Agreement

This Agreement made this _____ day of _____ 2020, by and between CPC established by an Act of Parliament namely Act No. 28 of 1961 & having its registered Office at 609, Dr. Danister De Silva Mawatha, Colombo 09 in the Government of the Democratic Socialist Republic of Sri Lanka (hereinafter called and referred to as the "CPC" which terms of expression as herein used shall where this context so requires and admits mean & include the CPC & its Successors & assigns) of the one part and _____ of _____ a Company duly incorporated & having its registered Office at _____ (hereinafter called the "Agent" which terms of expression as herein used shall where this context so requires and admits mean & include the _____ & its successors & assigns) of the other part

Whereas the CPC is desirous that the goods known as the Anti-Virus Solution for CPC for three years period should be supplied by the Supplier, and has accepted a Bid by the Supplier for the supply of such Goods and the remedying of any defects therein.

The CPC and the Agent agree, as follows: -

1. In the agreement words and expressions shall have the same meanings as are respectively assigned to them in the Conditions of Contract and Contractor's scope of work hereinafter referred to.
2. The following documents shall be deemed to form and be read and construed as a part of this Agreement.
 - **Letter of Acceptance dated _____.**
 - **The Bid dated _____.**
 - **The Conditions of Contract**
 - **Technical Specifications**
 - **The Completed Schedule of prices and**
 - **The Local Agent's Proposal**

3. In consideration of the payments to be made by the CPC to the Agent as hereinafter mentioned, the Agent hereby covenants with the CPC to supply and remedy any defects therein, fit for purpose in conformity in all respect according to the provisions of the Agreement..

4. The CPC hereby covenants to pay the Agent in consideration of the Supply and the remedying of defects therein, the agreed Price or such other sum as may become payable under the provisions of the Contract at the times and in the manner prescribed by the Agreement.

In Witness whereof the parties have hereunto caused this Agreement to be executed the day, month & year afore written.

Authorized Signature of the Chairman of CPC		Authorized Signature of the Supplier	
<u>In the presence of</u>		<u>In the presence of</u>	
Name		Name	
Signature		Signature	
Address		Address	

ANNEXURE - D - Format for Performance Guarantee

.....[issuing Agency's Name and Address of issuing Branch or Office].....

Beneficiary :[Name and Address of Employer]
.....

Date :

PERFORMANCE GUARANTEE NO :

We have been informed that[name of Contractor/ Supplier] (hereinafter called "the Contractor") has entered into Contract No.[reference number of the contract] datedwith you, for the [insert " construction"/ "Supply"] of[name of contract and brief description of Works] (hereinafter called "the Contract")

Furthermore, we understand that, according to the conditions of the Contract, a performance guarantee is required.

At the request of the Contractor, we [name of Agency] hereby irrevocably undertake to pay you any sum or sums not exceeding in total an amount of[amount in figures] (.....) [amount in words], such sum being payable in the types and proportions of currencies in which the Contract Price is payable, upon receipt by us of your first demand in writing accompanied by a written statement stating that the Contractor is in breach of its obligation(s) under the Contract, without your needing to prove or to show grounds for your demand or the sum specified therein.

This guarantee shall expire, no later than theday of, 2020 [insert date, 28 days beyond the scheduled contract completion date] and any demand for payment under it must be received by us at this office on or before that date.

This guarantee shall be governed by the laws of Sri Lanka and shall be subject to the Uniform Rules for Demand Guarantees, published as number 758 by the International Chamber of Commerce, except as stated above.

.....
[Signature(s)]