LBP LEASING AND FINANCE CORPORATION
(A LANDBANK Subsidiary)
15th Floor SycipLaw Centre Bldg, #105 Paseo de Roxas St. 1226 Makati City
Telephone Number 8818-2200/ Fax Number 819-6176

INVITATION TO QUOTE FOR PROCUREMENT OF ENDPOINT SECURITY SOLUTION
(LLFC-CAP-25-026)

REQUEST FOR QUOTATION (Small Value Procurement)

LBP Leasing and Finance Corporation (LLFC) through its Bids and Awards Committee (BAC) will undertake a Small Value Procurement in accordance with Section 53.9 of the 2016 Revised Implementing Rules and Regulations of the Republic Act No. 9184.

Name of the Project	**Procurement of Endpoint Security Solution (LLFC-CAP-25-026)**
Approved Budget of the Contract (ABC)	**Five Hundred Thousand Pesos and 00/100 (PHP 500,000.00)**

BACKGROUND

The Corporation regularly updates its endpoint security as part of its standard cybersecurity practices to prevent unauthorized access and reduce exposure to various threats such as viruses, malware, phishing, and other malicious activities. While the current solution has provided baseline protection, the evolving threat landscape, growing organizational needs, and geopolitical considerations have prompted a reassessment. This ensures that the new endpoint security solution aligns with current regulatory standards and the organization's overall risk posture.

OBJECTIVES OF THE PROCUREMENT

The objective of this procurement is to acquire an Endpoint Security Solution that aligns with current regulatory standards and LLFC's overall risk posture.

SCOPE OF WORK

- **Quantity**: 130 units
- **Subscription Period:** One (1) Year / Twelve (12) Months
- **Supported Operating System:** Windows Server 2016 to 2022 (and Core), Windows 11 Update (23h2) and earlier, Windows 10 Update (22h2) and earlier, Windows 10 IoT Enterprise.
- Server license allowed up to 35% and Mailboxes for up to 150% of the total devices

Endpoint Protection

- The solution must have a local and cloud machine learning that provide predictive detection of unknown malware, dynamic file analysis trained on billions of samples, local machine learning trained on 80,000 malware features, and threat intelligence from over 500 million endpoints globally.
- Shall provide advanced anti-exploit that focuses on attack tools and techniques to detect both known and zero-day exploits that target browser and popular software applications.
- Shall provide fileless attack protection to detect and block fileless malware at pre-execution, including terminating PowerShell running malicious command line, blocking malicious traffic, analyzing memory buffer prior to code injection, and blocking the code injection process.
- Shall provide network attack defense that focuses on detecting network attacks designed to gain access on endpoints through specific techniques such as: brute-force attacks, network exploits, password stealers, drive-by-download infection vectors, bots, and trojans.
- Shall provide ransomware vaccine that immunizes machines against known ransomware blocking the encryption process even if the computer is infected.
- Shall provide ransomware mitigation that uses detection and remediation technologies to keep files from ransomware attack.
- Shall provide the capability to automatically create backup copies of the files up to 15 MB in size, or smaller and restores them to their original location in case of ransomware infection.
- The proposed solution must have a dedicated virtual machine that deduplicates and centralizes most of the antimalware functionality of antimalware agents, acting as a scan server.
- Shall provide a next-gen tunable machine learning technologies designed specifically to detect advanced attacks and suspicious activities in the pre-execution phase.
- Shall provide web threat protection that scans incoming web traffic, including SSL, HTTP and HTTPSs traffic, to prevent the download of malware to the endpoint. Automatically blocks phishing and fraudulent web pages. Displays search ratings signaling trusted and untrusted pages
- The solution shall prevent sensitive data leakage and malware infection on attached devices by applying rules and exclusions via policy such as block, allow, and via custom rules.

- The solution shall provide full visibility and control of running applications by blacklisting unwanted software. Helps limit the risk of malicious code running undetected.
- The solution shall provide fully-featured two-way firewall that controls applications access to the network and to the internet. Furthermore, the firewall can protect the system against port scans, restrict ICS and warn when new nodes join a Wi-Fi connection.
- The solutions shall provide data protection that allows blocking of confidential data (pin card, bank account, etc.) for both HTTP and SMTP, by creating specific rules.
- Shall provide protection against highly sophisticated cyber-attacks using multiple stage signature-less technologies.
- Shall provide layered architecture that includes endpoint visibility, controls, prevention, detection, and remediation.
- Shall provide process inspection that provides behavior-based real time detection; monitors all processes running in the operating system and if the process is deemed malicious, will terminate it.
- Must have integrated root cause analysis that highlights the attack vector, the attack entry point, and how the attack originated. Helps pinpoint the origin node of attack, highlighted in the Incident page. The confidence score provides context for security events.

Sandbox Analyzer

- The proposed solution must provide integrated sandbox analyzer to enhance targeted attack detection.
- Shall provide pre-execution detection of advance attacks by automatically sending files that require further analysis to cloud sandbox and taking remediation action based on the verdict.
- The Sandbox module will be able to automatically send files to the Sandbox from the manufacturer's cloud where they can be detonated" for an in-depth analysis.
- The Sandbox module includes two analysis options: only monitoring or blocking. In monitoring mode, the user will be able to access the desired file, while in blocking mode, the user will be blocked from running the file until the Sandbox in the manufacturer's cloud gives the verdict.
- The Sandbox module includes two types of remedial actions: default and safety. For the default action, it will be possible to set: only reporting, disinfection, deletion and quarantine. For the safety action, it will be possible to establish: deletion or quarantine.
- The Sandbox module also includes the possibility of manually sending files to the Sandbox from the manufacturer's cloud. Thus, if the administrator suspects a file to be malicious, he can manually send it to the Sandbox to be „detonated" and find out the verdict. Administrator will be able to send several files at once, with the possibility to specify whether they will be „detonated" individually or all at the same time.
- The Sandbox module can support „detonation" of the following types of files: Batch, CHM, DLL, EML, Flash SWF, HTML, HTML/script, HTML (Unicode), JAR (archive), JS, LNK, MHTML (doc), MHTML (ppt), MHTML (xls), Microsoft Excel, Microsoft PowerPoint, Microsoft Word, MZ/PE files (executable), PDF, PEF (executable), PIF (executable), RTF, SCR, URL (binary), VBE, VBS , WSF, WSH, WSH-VBS, XHTML.
- The previously mentioned files will be able to be detected correctly even if they are included in archives of the type: 7z, ACE, ALZip, ARJ, Bzip2, cpio, Gzip, LHA, Linux TAR, LZMA Compressed Archive, MS Cabinet, MSI, PKZIP, RAR , Unix Z, ZIP, ZIP (multivolume), ZOO, XZ.
- The proposed Sandbox analyzer must be the same brand as the proposed Endpoint
- Protection and manageable in the same console without the need for additional virtual/physical hardware and license.

Endpoint Risk Analytics (ERA)

- The proposed solution must provide integrated Endpoint Risk Analytics (ERA) that identifies, assesses, and remediates Windows endpoints weaknesses via security risk scans either on-demand or scheduled via policy, considering a vast number of indicators of risk.
- Shall provide the ability to scan your network with certain indicators of risk and obtain an overview of network risk status via Risk Management dashboard, available from the Cloud Management Console.
- Must have the ability to provide an overview of the company risk score and score evolution.
- Must have the ability to provide an overview of statistics broken down into misconfigurations, vulnerable applications, and affected devices.
- Must have the ability to provide a description of each indicator of risk and the recommended remediation actions.
- Must have the ability to provide a Risk Management Dashboard that provides an overview of your network security and risk assessment information such as
    - Company Risk Score
    - Health Industry Modifier
    - Score Over Time
    - Top Misconfigurations
    - Top Vulnerable Apps
    - Top User Behavior Risks
    - Servers by Severity
    - Workstations by Severity
    - Top Devices at Risk
    - Top Users by Behavior Risk
- Must have the ability to resolve certain security risks automatically from the Cloud Management Console, and view recommendations for endpoint exposure mitigation.
    - The proposed ERA must be the same brand as the proposed Endpoint Protection and manageable in the same console without the need for additional virtual/physical hardware and license.

Endpoint Detection and Response (EDR)

- The proposed solution must provide integrated Endpoint Detection and Response (EDR).
- The proposed solution shall be a unified platform for preventative protection, post-breach detection, automated investigation, and response.
- It shall offer pre and post compromise attact visibility, alert triage, investigation, advanced search, and one-click resolution capabilities.
- The proposed EDR solution must includes the collection of data and events related to each workstation, bringing detailed map of them as well as automatic actions and integration with the Sandbox module and the advanced security module.
- Must have the ability to evaluate the typical activity of an endpoint from the perspective of its security according to MITRE ("baselining") attack techniques and can report any deviation from this behavior in the form of an incident.

Third Party Rating, Evaluation, Compatibility, and other requirements

- The solution should be able to integrate with Microsoft Active Directory.
- The proposed solution must be in the Leaders Part of Forrester Wave™: Endpoint Security provider, Q4 2023 or later.
- The proposed solution must be in the Strong Performers or Leaders Part of Forrester Wave™: Extended Detection and Response Platform, Q2 2024.

- The proposed solution participates in annual MITRE ATT&CK Evaluations 2022 or later for EDR conducted by MITRE Engenuity ATT&CK Evaluations.
- The proposed solution must be a visionary player in the recent Gartner Magic Quadrant of 2024 for EPP.
- Shall provide the capability to retrieve and download quarantined files for further analysis to Sandbox Analyzer, from Windows, Linux, or macOS endpoints. The files available for download are restricted to 25MB each and have a maximum of 10 retrieved files per company.
- Shall provide the capability to grant power user rights to access and modify the policy applied on the endpoints without the need to access the management console.
- The administrator can customize installation packages including only desired modules: firewall, content control, device control, power user, EDR sensor.
- The proposed solution must allow downloading of full kit installer packages that don't requires an internet connection upon installation.
- The EDR module allows the filtering of incidents from the graphic interface depending on the time interval, based on a confidence score ("confidence score"), attack indicators, attack techniques (ATT&CK) respectively affected operating system as well as by IP, file name, station name.
- The EDR module provides full visibility on the techniques, tactics, and procedures (TTPs) being used in active attacks while providing comprehensive search capabilities for specific indicators of compromise (IoCs), MITRE ATT&CK techniques and other artifacts to discover early-stage attacks.
- The proposed EDR must be compatible with any pre-installed endpoint protection and will function as EDR (Report Only).
- The proposed EDR must be the same brand as the proposed Endpoint Protection and manageable in the same console without the need for additional virtual/physical hardware and license.

Unified Management Console

- The proposed solution must provide a single cloud-based centralized management console that manages the following proposed security features:
  - Endpoint Protection
  - Sandbox Analyzer
  - Endpoint Risk Analytics
  - Endpoint Detection and Response (EDR)
- The proposed solution must use a one-to-one license scheme and a transferable license wherein each endpoint device must have a dedicated license (1:1 ratio).
- The proposed solution should avoid kernel-mode deployment, utilize a lightweight agent instead, and allow staging to test new kits or updates in a controlled environment that mirrors production, helping identify issues before deployment.
- The solution must have built-in two-factor authentication (2FA) that works with authenticator apps (Google and Microsoft) and does not require additional hardware and license to setup.
- Must have the capability to add, remove, arrange, configure, and customize the dashboard report, and does not limit the IT admin to a fixed dashboard.
- Single policy template to manage the configuration of all the proposed security features.
- Policy can be automatically changed depending on:
  - IP or IP class of the station
  - The assigned gateway
  - Assigned DNS server.
  - WINS assigned server.
  - DNS suffix for DHCP connection
  - The client is/is not in the same network as the management infrastructure (the workstation can implicitly resolve the hostname)
  - Network type (LAN, wireless)
- Quarantined files can be stored for up to 180 days and can be remotely restored with a configurable location or deleted from the management console.

Supplier Maintenance and Support

- Have a reputable local vendor representative in the Philippines that has been active in cybersecurity trade for at least 10 years now.
- Supplier of the solution have at least two (2) certified engineers for end-point solution
- Able to provide 3-Tier support (1st local, 2nd Distributor and 3rd Principal)
- Provides regular call or email check-up for concerns and product health monitoring even after sales.
- Available support through phone, email, web-remote assistance and on-site/on-call support.
- The solution must be able to provide comprehensive after-sales agreement options
- Conducts quarterly preventive maintenance for endpoint protection
- Regular pattern updates and firmware upgrade in co-term with the years of subscription
- Includes installation and configuration
- Includes Knowledge Transfer with completion and configuration report. Onsite conducted by Certified Professional Engineer for product served
- Includes vulnerability assessment for one (1) server on quarterly basis for Windows/Linux operating system.
- Includes Cybersecurity Awareness Training (1-Day Virtual Session)

Delivery Period

- Fifteen (15) working days upon receipt of Purchase Order and Notice to Proceed (NTP).

1. Please accomplish the following:
   a.) Price Quotation Form (Annex "A") together with the supplier's official proposal/quotation
   b.) Statement of Compliance under Schedule of Requirements and Technical Specifications (Annex "B")
   c.) Original and notarized Omnibus Sworn Statement (Annex "C")
   d.) Notarized Secretary's Certificate for proof of authorization

Submit in a sealed envelope to LBP Leasing and Finance Corporation office located at 15th Floor, SyCip Law Centre Bldg, #105 Paseo de Roxas St., Makati City **on or before August 19, 2025 05:00PM** together with the **Certified True Copies** of the following **Eligibility documents**:

a.) Valid and current year Mayor's Permit
b.) Valid and current PhilGEPS Registration Number
c.) DTI/SEC Registration (for Partnership/Corporation)
d.) Latest Tax Clearance per E.O. 398, series of 2005

2. All quotations must include all applicable taxes and shall be valid for a period of thirty (30) calendar days from the deadline of submission of quotations. Quotations received in excess of the approved budget shall be automatically rejected.

3. Liquidated damages equivalent to one tenth (1/10) of the one percent (1%) of the value of Purchase Order not completed within the prescribed completion period shall be imposed per day to day of delay. LLFC may rescind the agreement once the cumulative amount of liquidated damages reaches ten percent (10%) of the amount of purchase order, without prejudice to other courses of action and remedies open to it.

4. The project shall be awarded to the proponent determined to have submitted the complete and lowest quotation including compliance with the Schedule of Requirements and Eligibility documents.

5. The prospective bidder shall be a Filipino citizen/sole proprietorship/partnership/Corporation duly organized under the laws of the Philippines.

6. LLFC reserves the right to reject any or all quotations at any time prior to award of the project without thereby incurring any liability to the affected proponents and to waive any minor defects therein to accept the quotation as may be considered more advantageous to the Government.

7. Payment shall be within thirty (30) calendar days from date of acceptance. The procurement of LLFC is subject to a final VAT withholding of five percent (5%) in addition to the applicable withholding tax.

For further information, please visit LBP Leasing and Finance Corporation office or contact the BAC Secretariat Mr. Jose Emmanuel I. Guerrero at telephone number 8818-2200 loc. 231 or send e-mail to procurement@lbpleasing.com

Date of issue: 13 August 2025

(Sgd.)
MS. RIZA M. HERNANDEZ
CHAIRPERSON
BIDS AND AWARDS COMMITTEE

Annex "A"

Price Quotation Form

Date:

MS. RIZA M. HERNANDEZ
Chairperson, Bids and Awards Committee
LBP Leasing and Finance Corporation (LLFC)
15th Flr., Sycip Law Center, #105 Paseo de Roxas St.,
Makati City

Dear **Ms.. Hernandez**:

After having carefully read and accepted the terms and conditions in the Request for Quotation (RFQ), hereunder is our quotation/s for the item/s as follows:

Description/ Specifications:	Qty.	Unit Price (P)	Total Price (P)
(In details)			
Amount in Words:_____			
Warranty			

The above-quoted prices are inclusive of all costs and applicable taxes. Delivery **to LBP Leasing and Finance Corporation** shall not later than fifteen (15) calendar days upon receipt of Purchase Order (P.O.) and Notice to Proceed.

Very truly yours,

_____
Printed Name over Signature of Authorized Representative

_____
Name of Company

_____
Contact No./s

Please submit all the required eligibility documents together with the Annexes "A, B and C"

Schedule of Requirements and Eligibility Requirements

Bidders must state **"Comply"** in the column "Statement of Compliance" against each of the individual parameters.

Requirements	Statement of Compliance
• **Quantity**: 130 units • **Subscription Period:** One (1) Year / Twelve (12) Months • **Supported Operating System:** Windows Server 2016 to 2022 (and Core), Windows 11 Update (23h2) and earlier, Windows 10 Update (22h2) and earlier, Windows 10 IoT Enterprise. • Server license allowed up to 35% and Mailboxes for up to 150% of the total devices	
Endpoint Protection • The solution must have a local and cloud machine learning that provide predictive detection of unknown malware, dynamic file analysis trained on billions of samples, local machine learning trained on 80,000 malware features, and threat intelligence from over 500 million endpoints globally. • Shall provide advanced anti-exploit that focuses on attack tools and techniques to detect both known and zero-day exploits that target browser and popular software applications. • Shall provide fileless attack protection to detect and block fileless malware at pre-execution, including terminating PowerShell running malicious command line, blocking malicious traffic, analyzing memory buffer prior to code injection, and blocking the code injection process. • Shall provide network attack defense that focuses on detecting network attacks designed to gain access on endpoints through specific techniques such as: brute-force attacks, network exploits, password stealers, drive-by-download infection vectors, bots, and trojans. • Shall provide ransomware vaccine that immunizes machines against known ransomware blocking the encryption process even if the computer is infected. • Shall provide ransomware mitigation that uses detection and remediation technologies to keep files from ransomware attack. • Shall provide the capability to automatically create backup copies of the files up to 15 MB in size, or smaller and restores them to their original location in case of ransomware infection. • The proposed solution must have a dedicated virtual machine that deduplicates and centralizes most of the antimalware functionality of antimalware agents, acting as a scan server. • Shall provide a next-gen tunable machine learning technologies designed specifically to detect advanced attacks and suspicious activities in the pre-execution phase. • Shall provide web threat protection that scans incoming web traffic, including SSL, HTTP and HTTPSs traffic, to prevent the download of malware to the endpoint. Automatically blocks phishing and fraudulent web pages. Displays search ratings signaling trusted and untrusted pages • The solution shall prevent sensitive data leakage and malware infection on attached devices by applying rules and exclusions via policy such as block, allow, and via custom rules. • The solution shall provide full visibility and control of running applications by blacklisting unwanted software. Helps limit the risk of malicious code running undetected. • The solution shall provide fully-featured two-way firewall that controls applications access to the network and to the internet. Furthermore, the firewall can protect the system against port scans, restrict ICS and warn when new nodes join a Wi-Fi connection. • The solutions shall provide data protection that allows blocking of confidential data (pin card, bank account, etc.) for both HTTP and SMTP, by creating specific rules. • Shall provide protection against highly sophisticated cyber-attacks using multiple stage signature-less technologies. • Shall provide layered architecture that includes endpoint visibility, controls, prevention, detection, and remediation. • Shall provide process inspection that provides behavior-based real time detection; monitors all processes running in the operating system and if the process is deemed malicious, will terminate it. • Must have integrated root cause analysis that highlights the attack vector, the attack entry point, and how the attack originated. Helps pinpoint the origin node of attack, highlighted in the Incident page. The confidence score provides context for security events.	
Sandbox Analyzer • The proposed solution must provide integrated sandbox analyzer to enhance targeted attack detection. • Shall provide pre-execution detection of advance attacks by automatically sending files that require further analysis to cloud sandbox and taking remediation action based on the verdict. • The Sandbox module will be able to automatically send files to the Sandbox from the manufacturer's cloud where they can be detonated" for an in-depth analysis. • The Sandbox module includes two analysis options: only monitoring or blocking. In monitoring mode, the user will be able to access the desired file, while in blocking mode, the user will be blocked from running the file until the Sandbox in the manufacturer's cloud gives the verdict. • The Sandbox module includes two types of remedial actions: default and safety. For the default action, it will be possible to set: only reporting, disinfection, deletion and quarantine. For the safety action, it will be possible to establish: deletion or quarantine. • The Sandbox module also includes the possibility of manually sending files to the Sandbox from the manufacturer's cloud. Thus, if the administrator suspects a file to be malicious, he can manually send it to the Sandbox to be „detonated" and find out the verdict. Administrator will be able to send several files at once, with the possibility to specify whether they will be „detonated" individually or all at the same time. • The Sandbox module can support „detonation" of the following types of files: Batch, CHM, DLL, EML, Flash SWF, HTML, HTML/script, HTML (Unicode), JAR (archive), JS, LNK, MHTML (doc), MHTML (ppt), MHTML (xls),	

Microsoft Excel, Microsoft PowerPoint, Microsoft Word, MZ/PE files (executable), PDF, PEF (executable), PIF (executable), RTF, SCR, URL (binary), VBE, VBS , WSF, WSH, WSH-VBS, XHTML. • The previously mentioned files will be able to be detected correctly even if they are included in archives of the type: 7z, ACE, ALZip, ARJ, Bzip2, cpio, Gzip, LHA, Linux TAR, LZMA Compressed Archive, MS Cabinet, MSI, PKZIP, RAR , Unix Z, ZIP, ZIP (multivolume), ZOO, XZ. • The proposed Sandbox analyzer must be the same brand as the proposed Endpoint • Protection and manageable in the same console without the need for additional virtual/physical hardware and license.	
Endpoint Risk Analytics (ERA) • The proposed solution must provide integrated Endpoint Risk Analytics (ERA) that identifies, assesses, and remediates Windows endpoints weaknesses via security risk scans either on-demand or scheduled via policy, considering a vast number of indicators of risk. • Shall provide the ability to scan your network with certain indicators of risk and obtain an overview of network risk status via Risk Management dashboard, available from the Cloud Management Console. • Must have the ability to provide an overview of the company risk score and score evolution. • Must have the ability to provide an overview of statistics broken down into misconfigurations, vulnerable applications, and affected devices. • Must have the ability to provide a description of each indicator of risk and the recommended remediation actions. • Must have the ability to provide a Risk Management Dashboard that provides an overview of your network security and risk assessment information such as o Company Risk Score o Health Industry Modifier o Score Over Time o Top Misconfigurations o Top Vulnerable Apps o Top User Behavior Risks o Servers by Severity o Workstations by Severity o Top Devices at Risk o Top Users by Behavior Risk • Must have the ability to resolve certain security risks automatically from the Cloud Management Console, and view recommendations for endpoint exposure mitigation. o The proposed ERA must be the same brand as the proposed Endpoint Protection and manageable in the same console without the need for additional virtual/physical hardware and license.	
Endpoint Detection and Response (EDR) • The proposed solution must provide integrated Endpoint Detection and Response (EDR). • The proposed solution shall be a unified platform for preventative protection, post-breach detection, automated investigation, and response. • It shall offer pre and post compromise attact visibility, alert triage, investigation, advanced search, and one-click resolution capabilities. • The proposed EDR solution must includes the collection of data and events related to each workstation, bringing detailed map of them as well as automatic actions and integration with the Sandbox module and the advanced security module. • Must have the ability to evaluate the typical activity of an endpoint from the perspective of its security according to MITRE (“baselining”) attack techniques and can report any deviation from this behavior in the form of an incident.	
Third Party Rating, Evaluation, Compatibility, and other requirements • The solution should be able to integrate with Microsoft Active Directory. • The proposed solution must be in the Leaders Part of Forrester Wave™: Endpoint Security provider, Q4 2023 or later. • The proposed solution must be in the Strong Performers or Leaders Part of Forrester Wave™: Extended Detection and Response Platform, Q2 2024. • The proposed solution participates in annual MITRE ATT&CK Evaluations 2022 or later for EDR conducted by MITRE Engenuity ATT&CK Evaluations. • The proposed solution must be a visionary player in the recent Gartner Magic Quadrant of 2024 for EPP. • Shall provide the capability to retrieve and download quarantined files for further analysis to Sandbox Analyzer, from Windows, Linux, or macOS endpoints. The files available for download are restricted to 25MB each and have a maximum of 10 retrieved files per company. • Shall provide the capability to grant power user rights to access and modify the policy applied on the endpoints without the need to access the management console. • The administrator can customize installation packages including only desired modules: firewall, content control, device control, power user, EDR sensor. • The proposed solution must allow downloading of full kit installer packages that don’t requires an internet connection upon installation. • The EDR module allows the filtering of incidents from the graphic interface depending on the time interval, based on a confidence score ("confidence score"), attack indicators, attack techniques (ATT&CK) respectively affected operating system as well as by IP, file name, station name. • The EDR module provides full visibility on the techniques, tactics, and procedures (TTPs) being used in active attacks while providing comprehensive search capabilities for specific indicators of compromise (IoCs), MITRE ATT&CK techniques and other artifacts to discover early-stage attacks. • The proposed EDR must be compatible with any pre-installed endpoint protection and will function as EDR (Report Only). • The proposed EDR must be the same brand as the proposed Endpoint Protection and manageable in the same console without the need for additional virtual/physical hardware and license.	
Unified Management Console • The proposed solution must provide a single cloud-based centralized management console that manages the following proposed security features:	

○ Endpoint Protection ○ Sandbox Analyzer ○ Endpoint Risk Analytics ○ Endpoint Detection and Response (EDR) • The proposed solution must use a one-to-one license scheme and a transferable license wherein each endpoint device must have a dedicated license (1:1 ratio). • The proposed solution should avoid kernel-mode deployment, utilize a lightweight agent instead, and allow staging to test new kits or updates in a controlled environment that mirrors production, helping identify issues before deployment. • The solution must have built-in two-factor authentication (2FA) that works with authenticator apps (Google and Microsoft) and does not require additional hardware and license to setup. • Must have the capability to add, remove, arrange, configure, and customize the dashboard report, and does not limit the IT admin to a fixed dashboard. • Single policy template to manage the configuration of all the proposed security features. • Policy can be automatically changed depending on: ○ IP or IP class of the station ○ The assigned gateway ○ Assigned DNS server. ○ WINS assigned server. ○ DNS suffix for DHCP connection ○ The client is/is not in the same network as the management infrastructure (the workstation can implicitly resolve the hostname) ○ Network type (LAN, wireless) • Quarantined files can be stored for up to 180 days and can be remotely restored with a configurable location or deleted from the management console.	
Supplier Maintenance and Support • Have a reputable local vendor representative in the Philippines that has been active in cybersecurity trade for at least 10 years now. • Supplier of the solution have at least two (2) certified engineers for end-point solution • Able to provide 3-Tier support (1st local, 2nd Distributor and 3rd Principal) • Provides regular call or email check-up for concerns and product health monitoring even after sales. • Available support through phone, email, web-remote assistance and on-site/on-call support. • The solution must be able to provide comprehensive after-sales agreement options • Conducts quarterly preventive maintenance for endpoint protection • Regular pattern updates and firmware upgrade in co-term with the years of subscription • Includes installation and configuration • Includes Knowledge Transfer with completion and configuration report. Onsite conducted by Certified Professional Engineer for product served • Includes vulnerability assessment for one (1) server on quarterly basis for Windows/Linux operating system. • Includes Cybersecurity Awareness Training (1-Day Virtual Session)	
Delivery Period • Fifteen (15) working days upon receipt of Purchase Order and Notice to Proceed (NTP)	
Eligibility Requirements *(Certified True Copies only)* :	
1. Valid and Current Year Mayor's Permit or proof of application	
2. Valid and Current PhilGEPS Registration Number	
3. DTI / SEC Registration (for Partnership / Corporations)	
4. Latest Tax Clearance per E.O. 398, series of 2005	
5. Notarized Omnibus Sworn Statement (Annex C)	
6. Notarized Secretary's Certificate for proof of authorization	

I hereby certify to comply and deliver all the above Schedule of Requirements.

Name of Company /Bidder	**Signature over Printed Name of Authorized Representative**	**Date**

Annex "C"

Omnibus Sworn Statement

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

A F F I D A V I T

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;

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 following responsibilities as a Bidder:

   a) Carefully examine all of the Bidding Documents;

   b) Acknowledge all conditions, local or otherwise, affecting the implementation of the Contract;

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

   d) Inquire or secure 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.

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

_____

Bidder's Representative/Authorized Signatory

Annex "C"

SUBSCRIBED AND SWORN to before me this ___ day of *[month] [year]* at *[place of execution]*, Philippines. Affiant/s is/are personally known to me and was/were identified by me through competent evidence of identity as defined in the 2004 Rules on Notarial Practice (A.M. No. 02-8-13-SC). Affiant/s exhibited to me his/her [insert type of government identification card used], with his/her photograph and signature appearing thereon, with no. _____ and his/her Community Tax Certificate No. _____ issued on ____ at _____.

Witness my hand and seal this ___ day of *[month] [year]*.

NAME OF NOTARY PUBLIC
Serial No. of Commission _____
Notary Public for _____ until _____
Roll of Attorneys No. _____
PTR No. _____ *[date issued], [place issued]*
IBP No. _____ *[date issued], [place issued]*

Doc. No. _____
Page No. _____
Book No. _____
Series of _____

* This form will not apply for WB funded projects.