Republic of the Philippines
**Department of Agriculture**
**AGRICULTURAL CREDIT POLICY COUNCIL**
28/F One San Miguel Avenue (OSMA) Bldg.,
San Miguel Avenue corner Shaw Blvd.,
Ortigas Center 1605 Pasig City
Tel. Nos. 8634-3320 to 21; 8634-3326 / Fax Nos. 8634-3319; 8584-3691



Date: October 13, 2022
RFQ No. 2022 – 042

# REQUEST FOR QUOTATION (RFQ)

The Agricultural Credit Policy Council (ACPC) through its Bids and Awards Committee (BAC), intends to procure:

**PROCUREMENT OF ONE HUNDRED FIFTY (150) LICENSES OF ENDPOINT SECURITY SOLUTION**

| | | |
|---|---|---|
| Approved Budget for the Contact | : | PhP 450,000 |
| Purchase Request/s No | : | 2022-10-573 |
| Mode of Procurement | : | NP-Small Value Procurement (Sec. 53.9) |

Interested bidders/supplier of known qualifications are hereby invited to submit quotation signed by its authorized representative at the below address and/or thru email to the following addresses:

**Agricultural Credit Policy Council**
28F One San Miguel Ave. Building, San Miguel Ave. cor. Shaw Blvd., Ortigas Center, Pasig City

**Ma. Cathrina R. Pelagio**
BAC Secretariat
mcrpelagio@acpc.gov.ph

**Hanna Candy B. Gonzales**
BAC Secretariat
hcbgonzales@acpc.gov.ph

Supplier who will submit proposals with the **lowest calculated quotations shall be selected**. A copy of the following documentary requirements as prescribed in the IRR of RA 9184 for NP-Small Value Procurement (Sec 53.9) shall be submitted on or before **October 21, 2022 (Friday), 5PM.**

1. Mayor's/Business Permit
2. PhilGEPS Registration Certificate
3. DTI/SEC Registration
4. Latest Income Tax Return
5. Notarized Omnibus Sworn Statement

**INSTRUCTION TO SUPPLIER**

- Submit your quotation using the prescribed **Quotation Form** (Annex A of the RFQ).
- Accomplish the Quotation Form and do not alter the contents of the form in any way.
- Non-compliance with the submission of the **accomplished prescribed/standard Quotation Form** and **Documentary Requirements within the prescribed deadline** shall automatically be disqualified.

Very truly yours,

**DIR. MAGDALENA S. CASUGA**
BAC CHAIRPERSON

Rachel Bustamante (Oct 13, 2022 16:53 GMT+8)

**ANNEX A**

**QUOTATION FORM**

**Name of Company** : _____
**Address** : _____
**Contact Person** : _____
**Contact Number** : _____
**Email address** : _____
**TIN** : _____

After having carefully read and accepted the Terms and Conditions of this RFQ specified Annex B, hereunder is our quotation/s for the item as follows:

| Item No. | QTY/UNIT | Approved Budget for the Contract (ABC) | | Description and Technical Specifications | Supplier's Price Proposal (VAT Inclusive) | |
|---|---|---|---|---|---|---|
| | | Unit Price | Total Price | | Unit Price | Total Price |
| 1 | 150 licenses | ₱ 3,000 | ₱ 450,000 | **Cloud-based Endpoint Security Solutions**<br>- One (1) year subscription<br>- **Terms of Reference** *(Attached in Annex C)* | | |
| | | | | **** VAT Inclusive**** | | |
| | **Note:** *Kindly specify the brand and attached a brochure of the items offered.* | | | | **TOTAL:** | |

*I hereby certify to comply and deliver all the above requirements.*

_____
Signature over Printed Name

_____
Position and Designation

_____
Date

**ANNEX B**

**TERMS AND CONDITION**

**I. VALIDITY OF PRICE QUOTATIONS AND OTHER IMPORTANT REMINDERS**

- Price quotation/s, to be denominated in Philippine peso shall include all taxes, duties and/or levies Payable.
- Price validity shall be valid for a period of thirty (30) calendar days from the date of submission.
- Warranty shall be for a minimum of three (3) months for supplies & materials; one (1) year for equipment, three (3) years for IT equipment from date of acceptance by the end-user.
- Quotations exceeding the Approved Budget for the Contract shall be rejected.
- The bidders are required to submit brochures, pictures and technical data pertaining to the brand and model of the item being offered.
- In case two or more bidders are determined to have submitted the Lowest Calculated Quotation, ACPC shall adopt a tie-breaking method to finally determine the single winning provider in accordance with GPPB Circular 06-2005.
- Award of Contract shall be made to the supplier/bidder with the lowest quotation and who has complied with the minimum technical specifications and other terms and conditions stated herein.

**II. DOCUMENTARY REQUIREMENTS**

The following Eligibility Requirement must be submitted along with your quotation:

a. Mayor's/Business Permit
b. PhilGEPS Registration Certificate
c. SEC/DTI Registration
d. Latest Income Tax Return
e. Omnibus Sworn Statement

**III. DELIVERY SCHEDULE AND ACCEPTANCE**

- Delivery period must be within **thirty (30) calendar days** upon receipt of the approved Purchase Order.
- The items shall be delivered according to the requirements specified herein.
- ACPC shall have the right to inspect and/or to test the goods to confirm their conformity to the specifications. Supplier shall, within 3 calendar days from notice, replace all defective items at no cost to the ACPC.

**IV. PAYMENT TERMS AND LIQUIDATED DAMAGES**

- Payment shall only be processed after the submission of billing statement/invoice and upon completion of delivery of all services listed in the Purchase Order/ Contract as well as upon inspection and acceptance of the goods by the end-user.

| **PAYMENT DETAILS:** | |
|---|---|
| **Banking Institution:** | |
| **Account Number:** | |
| **Account Name:** | |
| **Branch** | |

- Liquidated damages equivalent to one tenth of one percent (0.1%) of the value of the goods not delivered within the prescribed delivery period shall be imposed per day of delay.

**V. DEADLINE OF SUBMISSION**

- Quotations duly signed by the supplier's authorized representative should be submitted to the **BAC Secretariat** not later than **October 21, 2022 (Friday), 5PM** through a sealed envelope at the ACPC office in 28F One San Miguel Ave. Building, San Miguel Ave. cor. Shaw Blvd., Ortigas Center, Pasig City or through email. Quotations submitted after the said deadline shall not be accepted and considered. Any erasures or overwriting shall be valid only if these are signed or initialed by the bidder or his/her authorized representative/s.

I hereby declare that I understand and acknowledge the terms and conditions listed.

_____
Signature over Printed Name

_____
Position and Designation

_____
Date

**Annex C**

**Terms of Reference for Cloud-based Endpoint Security Solutions**

**I. General Objective**

The client intends to subscribe to an effective, reliable and comprehensive antivirus software solution that is easy to manage, cost effective, has proven protection and light on the system.

**II. Features, Specifications, Technical Capabilities and Benefits**

| Endpoint Protection | | |
|---|---|---|
| **Features** | Benefits | **Statement of Compliance** |
| **Supported Operating Systems** | Microsoft® Windows® 11/10/8.1/8 | |
| | Linux (version 7 and later) | |
| | Mac OS 10.12 and later | |
| | Android 5 (Lollipop) and later | |
| | iOS 8 and later | |
| **3rd Party Antivirus Software Removal** | The solution must have a mechanism to remove any other security solution present in the endpoint. This mechanism must be:<br>1. Integrated to the security solution<br>2. Provided as a standalone tool<br>3. Available through the centralized administration console | |
| **Modular installation** | The solution must allow to select which protection modules to install. For example:<br>1. Device Control<br>2. Firewall<br>3. Web Control | |
| **Password Protected Settings** | During the installation process, the solution must request the administrator to set a security password to protect the program settings in order to avoid any unauthorized modification. | |
| **Override Mode** | Must allow users on the client-computer level to change settings in the installed product, even if there is a policy applied over these settings. | |
| **Scanning options** | The solution must have at least the following scanning options:<br>1. Smart Scanning (the default set of targets for scanning and scanning optimizations) | |
| | 2. Custom Scanning (Custom scan lets you specify scanning parameters such as scan targets and scanning methods. Configurations can be saved to user-defined scan profiles, which can be useful if scanning is repeatedly performed with the same parameters.) | |
| | 3. Removable Media Scanning (Quickly launch a scan of removable media such as CD/DVD/USB that are currently connected to the computer.) | |
| | 4. Perform Last Used Scan (Quickly launch the previously performed scan using the same settings it was run with.) | |
| | The solution must have an option for WMI and Full Registry Scan to improve the registry scanning that can discover and eliminate malicious references or dangerous content anywhere in the registry or WMI repository | |
| **Malware Detection** | The solution must be able to detect all types of threats, including the most common ones: i.e., viruses, worms, Trojans, spyware, adware, rootkits, bots, ransomware, etc. | |
| | The solution must use multi-layered technologies - with the combination of virus signature database, generic signature database, code analysis, emulation, machine learning, cloud-powered scanning, sandbox technology - for superior malware detection capability. | |
| | The solution must be able to detect the following types of applications:<br>1. Potentially Unwanted Applications<br>2. Potentially Unsafe Applications<br>3. Suspicious Applications | |
| | The solution must include the following mechanisms for threat detection:<br>1. Real-Time Detection<br>2. Web-Access Detection<br>3. Email Detection<br>4. On-Demand Detection | |
| | Upon detecting a threat, the solution must offer the following actions:<br>1. Clean<br>2. Send to Quarantine<br>3. Submit to Vendor for Analysis<br>4. Exclude from Detection | |
| | When working in virtualized environments, the solution must be able to create a whitelist of safe files that can be shared within the virtual network. | |
| | The solution must offer the option to scan the files when performing any of the following actions:<br>1. Open<br>2. Create<br>3. Run<br>4. Copy | |
| **Idle-state Scanning** | The solution must run a Scheduled Scan when detecting any of the following states on the computer:<br>1. Active Screensaver<br>2. Session Lock<br>3. User Logoff | |
| **Device Control** | The solution must be able to control the following devices:<br>1. Mass storage devices (HDD, USB drives, etc.)<br>2. CDs/DVDs<br>3. USB connected printers<br>4. FireWire storage<br>5. Bluetooth devices<br>6. Card readers<br>7. Modems<br>8. LPT/COM ports | |
| | The solution must be able to allow or deny the use of devices based on the following criteria:<br>1. Provider (Manufacturer)<br>2. Model<br>3. Serial Number | |
| | The solution must be able to define a list of users that specifies who can access and use the devices. | |
| | For storage devices, the solution must allow to set up the following use permissions:<br>1. Read/Write<br>2. Block<br>3. Read Only<br>4. Warn | |
| | The solution must allow blocking of certain devices at specific period only. | |
| | When connecting a storage device or using a removable media, the solution must provide the following options:<br>1. Scan<br>2. No Action<br>3. Remember This Action | |

| | | |
|---|---|---|
| **Host-based Intrusion Prevention System (HIPS)** | The solution must have a Host-Based Intrusion Prevention System (HIPS). The HIPS system must have the following modes:<br>1. Automatic Mode<br>2. Smart Mode<br>3. Interactive Mode<br>4. Policy-Based Mode<br>5. Learning Mode | |
| **Advanced Memory Scanner** | The solution must have an Advanced Memory Scanner module to detect the most complex threats that have been designed to bypass the traditional detection mechanisms. | |
| **Exploit Blocker** | The solution must have an Exploit Blocker module to prevent exploitation of vulnerabilities in common applications such as:<br>1. Web browsers<br>2. PDF readers<br>3. Email clients<br>4. MS Office components | |
| **Machine Learning** | The solution must have combined power of neural networks (such as deep learning and long short-term memory) and a handpicked group of six classification algorithms. This allows it to generate a consolidated output and help correctly label the incoming sample as clean, potentially unwanted or malicious. | |
| **DNA Detection** | The solution must have the capability to detect types range from very specific hashes, which are complex definitions of malicious behavior and malware characteristics. | |
| | The solution must be able to identify malicious code that can be easily modified or obfuscated by attackers, the behavior of objects cannot be changed so easily and DNA Detections are designed to take advantage of this principle | |
| **Ransomware Shield** | The solution must have additional layer protecting users from ransomware. The technology should be able to monitor and evaluate all executed applications based on their behavior and reputation. | |
| | The solution should be able to detect and block processes that resemble behavior of ransomware. | |
| | The solution must be able to detect malicious activities of ransomware or filecoders. The solution should be capable of blocking the application and stopping its processes, but must also be able to notify the user to block or allow it. | |
| **Native ARM64 build** | The solution must offer protection for an ARM64 build platform | |
| **Brute-Force Attack protection** | The solution must be able to inspects the content of network traffic and blocks attempts of password-guessing attacks. | |
| **In-product Sandbox with built-in Cloud-Sandboxing technology** | The solution must be able to identifying the real behavior hidden underneath the surface of obfuscated malware. Utilizing this technology, it emulate different components of computer hardware and software to execute a suspicious sample in an isolated virtualized environment. | |
| | The solution must have cloud-based sandboxing technology that adds a powerful layer of security to your endpoint protection. It detects and analyzes never-before-seen threats to protect against ransomware, targeted attacks, advanced persistent threats (APTs), zero days and other sophisticated malware. | |
| | The solution must run the collected sample through a full sandbox, simulating user behavior to trick anti-evasive techniques. | |
| | The solution must also perform a deep learning neural network to compare the behavior seen versus historical behavioral data. | |
| | The solution must perform different layers of unpacking, scanning, and detecting of samples submitted such as:<br>1. Advanced unpacking and scanning with experimental detections<br>2. Advanced machine learning detection - with emulation and code analysis<br>3. Experimental detection engine - extracted binaries and dumps<br>4. In-depth behavioral analysis - sandbox outputs with behavioral features extraction | |
| | The solution must allow a per-computer detailed policy configuration so the administrator can control what is sent and what should happen based on the receiving result. | |
| | The solution must allow the administrator to see who sent what and what the result was directly from the console. | |
| | The solution must also be compatible not just for endpoint detection but should also work for mail servers. | |
| | Granular Reports<br>- Must be able to generatee report based on the findings and results of testing. Must allow the user to use one of the pre-defined reports or make a custom one. | |
| **Host-based Firewall** | The solution must have an Endpoint Firewall to allow or deny connections based on any of the following modes:<br>1. Automatic Mode<br>2. Interactive Mode<br>3. Learning Mode<br>4. Policy-Based Mode | |
| | The solution must allow configuration of settings such as:<br>1. Block all traffic<br>2. Pause all traffic (Allow all traffic) | |
| **Botnet Protection** | The solution must have a Botnet Protection module, which must be able to detect connections to malicious C&C servers and identify the typical behavior of computers that are part of a Botnet. | |
| **Email Protection** | The solution must protect all email communications made through any of the following protocols:<br>1. POP3<br>2. IMAP<br>3. HTTP<br>4. MAPI | |
| | The solution must be able to export emails in the following states:<br>1. Received<br>2. Sent<br>3. Read | |
| | In case of detecting a compromised email message, it must provide the following options:<br>1. Delete Email<br>2. Move Email to the Deleted Items Folder<br>3. Move Email to Custom Folder<br>4. No Action | |
| **Anti-spam Protection** | The solution must be able to verify communications using SSL protocols. | |
| | The solution must have an integrated Antispam Protection module. | |
| | The solution must be able to create blacklists and whitelists with emails. | |
| **Web Content Protection** | The solution must have a module that allows to define which websites can or cannot be accessed by the organization's employees. This module must allow to select a specific URL or a whole category of websites, such as:<br>1. Adult content<br>2. Social networks<br>3. Streaming services | |

| | | |
|---|---|---|
| | 4. Communications<br>5. Online games | |
| | The solution must allow blocking of certain websites at specific period only. | |
| | The solution must allow to exclude certain websites from being blocked. | |
| **Secure Browser** | The solution must have additional layer of protection designed to protect your sensitive data while browsing online (for example, financial data during online transactions). Enpoint protection contains a built-in list of predefined websites that will trigger a protected browser to open. | |
| | The solution must have protection for supported web-browser against other processing running on the computer. | |
| | Zero-trust approach and assumes that the computer or its protection capabilities are compromised or insufficient and does not allow to tamper with the browser's memory space and consequently with the content of the browser window. | |
| | Feature should not active by default so that administrators have enough time to leverage the potential in their security policies | |
| **Anti-Phishing Protection** | Protects your privacy and assets against attempts by fake websites to acquire sensitive information | |
| **Connected Networks** | Must be able to show the networks to which network adapters are connected. | |
| **System Inspector** | Must contain an application that thoroughly inspects the computer and gathers detailed information about system components such as drivers and applications, network connections or important registry entries and assesses the risk level of each component. | |
| | It must be able to display the following information about created logs: | |
| | Time – The time of log creation.<br>Comment – A short comment.<br>User – The name of the user who created the log.<br>Status – The status of log creation. | |
| **Unified Extensible Firmware Interface Scanner** | Must be able to detect malicious components in the firmware | |
| **Exclusion** | The solution must be able to exclude files from scanning using file extensions. | |
| **Network Attack Protection** | Must be able to detect known vulnerabilities in the network level | |
| **Intrusion Detection** | The solution must be able to detect and block various security problems in SMB protocol, namely:<br>Rogue server challenge attack authentication detection | |
| | IDS evasion during named pipe opening detection | |
| | CVE detections (Common Vulnerabilities and Exposures) | |
| | Must be able to detect and block various CVEs in the remote procedure call system developed for the Distributed Computing Environment (DCE) | |
| | Must be able to detect ARP poisoning attacks triggered by man in the middle attacks or detection of sniffing at network switch | |
| | Must be able to detect and block various CVEs in the RDP protocol | |
| | Must be able to prevent attacks that exploit the weaknesses of the ICMP protocol, which could lead to computer unresponsiveness | |
| | The solution allows for detection of DNS poisoning – relieving a fake answer to a DNS request (sent by an attacker) which can point you to fake and malicious websites | |
| | Must be able to detect attacks of port scanning software – application designed to probe a host for open ports by sending client requests to a range of port addresses with the goal of finding active ports and exploiting the vulnerability of the service. | |
| | The solution must be able to block unsafe address after attack detection | |
| **Detection Database Options** | The solution must be able to reverse to its previous detection database upon any case of false positive. | |
| | The solution must be able to create a local folder to manage updates in a centralized way. | |
| **Document Protection** | The solution must be able to scan Microsoft Office documents before they are opened, as well as files downloaded automatically by Internet Explorer such as Microsoft ActiveX elements | |
| **Cloud based reputation database** | The solution must have a technology capable of comparing files based on a whitelist that works with a file reputation database. | |
| | When inspecting an object such as a file or URL, before any scanning takes place the solution must be able to check the local cache for known malicious or whitelisted benign objects. | |
| **Micro Program Component Update (Feature update)** | The solution must have a reducing network bandwidth usage when updating antivirus.<br>- MicroPCU can wait for a reboot for weeks<br>- Does not reinstall the product with all downsides like deregistering from the system during the process, including configuration transfer<br>- Downloads less data (differential update)<br>- comes with a friendly or completely suppressible reminder for the user and is compatible with managed networks | |
| **Transparent mode** | The solution must have a Transparent mode that shows no warnings whenever a full-screen application is running. | |
| **Encryption** | | |
| **Features** | Benefits | **Statement of Compliance** |
| **Endpoint Encryption** | The solution must provide additional security to the machine: | |
| | 1. Encrypt system disks, partitions or entire drives | |
| | 2. Cross platform coverage (MacOS and Windows) | |
| | 3. Single click deployment | |
| | The encryption solution must use the industry-recognized FIPS 140-2 validated 256 bit AES encryption standard for assured security | |
| **Management Console** | | |
| **Features** | Benefits | **Statement of Compliance** |
| **Supported Browsers (Cloud-based console)** | Cloud-based console must be able to support the following browsers:<br>1. Mozilla Firefox | |
| | 2. Microsoft Edge | |
| | 3. Google Chrome | |
| | 4. Safari | |
| | 5. Opera | |
| **User Interface** | User interface muust include the following:<br>- Protection status icon<br>- Graphical user interface (new colors, icons, and navigation)<br>- Hide GUI completely<br>- Enhanced VDI Support<br>- Dark theme<br>- Presentation mode<br>- Quick links<br>- Native right-to-left (RTL) language support<br>- Touch screen support<br>- High resolution display support<br>- Re-engineered advanced settings<br>- Support for locally managed lists | |
| **Endpoint Detection and Communication** | The server must communicate with the endpoints through an agent that is capable of storing policies and run tasks while the computer is offline. | |
| | The server must have a module that detects traces of computers on the network and allows to perform actions on the detected computers. | |

| | | |
|---|---|---|
| **Endpoint Detection and Communication** | The server must have an MDM module that allows to connect and manage the mobile devices within the network. Both Android and iOS support is required. | |
| | The web console interface must work with informative dashboards. These have to be fully interactive and allow to carry out certain tasks from multiple sections. | |
| **Mobile Device Management and Security** | The management server must be able to enroll the devices from the following options:<br>1. Enrollment via email - mass enrollment via email of mobile devices that you do not have physical access to.<br>2. Individual enrollment via link or QR code - single mobile device enrollment. | |
| | MDM for Android should allow the administrator to monitor pre-defined device settings to determine if they are in compliance. The admin can monitor memory usage, Wi-Fi connection, data roaming, call roaming, unknown sources – other than Google Play store – USB debug mode, NFC and internal storage encryption, and their current state. | |
| | MDM for Android should allow the administrator to do the following security measures:<br>1. Define password complexity requirements.<br>2. Set maximum unlock attempts, after which the device will automatically go to factory settings.<br>3. Set maximum screen lock code age.<br>4. Set lock screen timer.<br>5. Prompt users to encrypt their mobile devices.<br>6. Block built-in camera usage. | |
| | MDM for Android should allow the administrator to manage the following application control settings:<br>1. Manually define applications to be blocked.<br>2. Category-based blocking - e.g. games, social media, etc.<br>3. Permission-based blocking - e.g. applications that track location, access contact lists, etc.<br>4. Blocking by source - applications installed from sources other than default app stores.<br>5. Set exceptions from the rules for blocked applications – whitelist applications.<br>6. Set a list of mandatory installed applications. | |
| | MDM for Android should allow the administrator to track, monitor and control applications and their access to personal/company data, sorted by categories. | |
| | MDM for Android should allow the administrator to send a custom message to a particular device or to a group of devices. The message is displayed in the form of a pop-up, so the user does not overlook it. | |
| | MDM for iOS should allow the administrator to create white/black lists of apps to prevent users from installing prohibited apps. Also,manage app notifications to users, including options for Notification Center, Sounds, Badge App Icon and others. | |
| | MDM for iOS should allow the administrator to manage the web content filtering settings. Adult web content, as defined by Apple, can be blocked. The administrator can also white/black-list specific URLs. | |
| | MDM for iOS should allow the administrator to significantly increase the security of your company's iOS devices by remotely pushing out security settings and restrictions of Passcode, iCloud, Privacy and others. | |
| | Enrolling devices should be flexible. It should allow mix and match of license seats. Migrate seats from one device to another, regardless of the OS. | |
| **Management Server capabilities** | The graphic interface informative dashboards have to allow the administrator to modify them in real time. | |
| | The web interface must be able to work with multiple tabs and allow the creation of more tabs manually if the administrator requires so. | |
| | The server must allow to add computers to the console using at least the following methods:<br>1. Active Directory synchronization<br>2. Entering computer name or IP address manually<br>3. Proprietary technology for detecting machines on the network | |
| | The server must allow remote installation of all its security solutions in a transparent way and without user intervention. | |
| | The server must allow the creation of static and dynamic groups for a better administration. | |
| | The server must allow visualization of the following computer information remotely:<br>1. Basic information<br>2. Configuration<br>3. Executed tasks<br>4. Installed applications<br>5. Alerts<br>6. Quarantine | |
| | Should be able to collect and display data about hardware information of endpoints connected to the security network. Data should include details such as: | |
| | CPU, RAM, monitors, disk drives, input devices and printers, including vendors, models, and serial numbers | |
| | Other hardware parameters should include:<br>Chassis, Device information, Display, Display adapter, Input device, Mass storage, Network adapter, Printer, Processor, RAM and Sound device | |
| **Reports and templates** | The server must provide a number of standard reports by default. | |
| | The server must allow the creation of new reporting templates with the possibility to choose from more than 200 data parameters. | |
| | Reports must be automatically sent by email or stored on the server if the administrator so requires. | |
| **Configuration and features** | The server must provide support for policy implementation on clients based on whether parameters are fulfilled or not. It must be possible to apply policies to individual computers or to a static or dynamic group. | |
| | The server must provide at least the following default tasks to facilitate computer administration:<br>1. On-Demand Scan<br>2. Export the security solution settings<br>3. Manage the quarantine folder<br>4. Update the detection database | |
| | The server must allow information messages to be sent to all types of workstations, including desktops, mobile devices, or tablets. | |
| | The server must allow the creation of multiple profiles for computer management. | |
| | Access profiles must be configured using different permissions for different tasks, for instance: Administrator, Report creators, Operators, etc. | |
| | The server must include a second authentication factor for access of users with more privileges. | |
| | The server must allow to export settings remotely to the managed computers. | |
| **Email Notification Settings** | The server should allow to configure email notification settings. It will have to provide the following standard notifications:<br>1.Malware propagation alert | |
| | 2. Network attack alert | |
| | 3. Outdated equipment alert | |
| | 4. Failed tasks alert | |
| **Low System Demands** | Delivers proven protection while leaving more system resources for programs you regularly use | |
| **III. Scope of Services: Product Training and Demonstration** | | **Statement of Compliance** |
| A. Conduct POC (Proof-of-Concept) activity to prove the compliance of the product | | |
| B. Conduct one (1) day product training and demonstration on deployment, configuration, administration, maintenance, and basic troubleshooting | | |
| C. Minimum of three (3) attendees | | |
| D. Includes training materials | | |

| IV. Scope of Services: Technical Support | Statement of Compliance |
|---|---|
| A. Standard Technical Support – 8x5 service assistance through email, phone, and remote desktop applications | |
| B. Provision of 8x5 onsite and on call services subject to confirmation by the helpdesk support | |
| C. Conduct health check activity on a quarterly basis | |
| D. Provide comprehensive Service Level Agreement duly signed by authorized representatives from the company, reseller, and the distributor | |
| **V. Awards and Recognitions** | **Statement of Compliance** |
| A. The solution must have a track record of doing cybersecurity for more than 30 years | |
| B. Received at least 100 VB100 Awards from Virus Bulletin | |
| C. Received at least 50 Advanced+ awards from AV Comparatives | |
| D. Must be a Challenger or a Leader in the latest Gartner Magic Quadrant | |

I hereby declare that I understand and acknowledge the terms and conditions listed.

Signature over Printed Name

Position and Designation

Date