TERMS OF REFERENCE (TOR)
FOR THE PROCUREMENT OF
ANTIVIRUS WITH ANTI RANSOMWARE
(CLOUD-BASED)

I. RATIONALE

Due to the large number of IT-based services that are required due to the implementation of various online services due to the global pandemic, the Quezon City LGU, which has an increasing number of servers and workstations requires protection from disruptive and destructive malware, including ransomware. Hence, the requirement for a new enterprise version of antimalware software is highly needed. Furthermore, due to limited cybersecurity skills of our IT personnel, skills will be augmented by a managed detection and response service coupled with Technical Training of our staff.

II. PROJECT DESCRIPTION

A cloud-based service covering 60 server licenses, 2000 workstation licenses, and integrated management - must have a unified console for managing multiple solution modules such as Advanced Endpoint Protection, Email Security, Server Security, anti-malware, command and control blocking, browser exploit protection, application control, behavior monitoring, ransomware protection, memory inspection, web threat protection, and vulnerability protection; Endpoint encryption ensures only authorized eyes can see your information; Light weight and optimized security ensures minimal impact on device, application, or network performance ;Updating the endpoints should have the ability to set pre-configured available bandwidth used for both software, Updating and threat definition updates (e.g. 64,128,256, kpbs etc.) Anti-rootkit Detection; Scanning; Advance deep Learning Mechanism; Advanced Exploit Prevention/Mitigation must detect and stop known exploits; Ability to integrate with existing firewall without additional subscription; Use machine learning technology to show prioritized list of the most suspicious files identified by EDR enabled services; Administrative Training/Knowledge Transfer for 5pax; Managed Detection and Response Service; Price is VAT inclusive.

A. WORKSTATION SECURITY

GENERAL FEATURES

Coverage: 2,000 Licenses for one year

- Endpoint Security Licenses with the following features:
    - Anti-malware
    - Application Control
    - Integrated Data Loss Prevention
    - Device Control

  - Email Security for Google Workspace
  - Web Reputation
  - Ransomware Rollback
  - Extended Detection and Response (XDR)

B. SERVER PROTECTION

GENERAL FEATURES

Coverage: 60 Licenses for one year

- The proposed solution provides self-defending servers; with multiple integrated modules below providing a line of defense at the server in a single agent :

  - Hosted Intrusion Detection System (HIPS)
    - Virtual Patching
  - Anti-Malware
  - Hosted Firewall
  - Integrity Monitoring
  - Log inspection
  - Application Control
  - Web Reputation
  - Support for Windows, Linux and Solaris OS
  - Extended Detection and Response (XDR) for Servers
  - With Yubikey

C. MANAGED DETECTION AND RESPONSE SERVICES

GENERAL FEATURES

Coverage: One year for 2,000 Endpoint licenses (including email and web Security) and 60 server licenses

- The provider shall provide 24 x 7 Continuous alert monitoring, correlation and prioritization using automation and analytics, and provide proactive sweeping of endpoint, server, and email.
- The service shall include the following:

  - Monitoring and Detection
  - Analysis and Investigation
  - Response and Reporting

- The Managed Service shall include the following:

  - Managed XDR for Endpoints Security
  - Manged XDR for Server Security
  - Premium Support Services

III. SCOPE OF WORK

- Installation and configuration of Cloud Based protection for 60 Servers licenses and 2000 workstation licenses inclusive of endpoint security, web reputation security, email security, and sandbox, all of which are of the same brand for ease of management
- Provision of 24 x 7 managed services from the manufacturer for the detection and response of 60 Server licenses and 2000 workstation licenses inclusive of web security, email security, and sandbox. The service shall include the following:
    - Monitoring and Detection
    - Analysis and Investigation
    - Response and Reporting
- The supplier must provide Security Health checks and Security Planning at least twice a year
- The Provider shall assign a dedicated Technical Account Manager to help leverage the deployed security solutions, optimize IT service levels and assist in the proactive security planning and provide crisis management planning assistance
- The service must include Security Planning twice a year

IV. AREA OF COVERAGE

The project covers the following IT Assets:

1. Endpoint Security Licenses with the following features:
    a. Anti-malware
    b. Application Control
    c. Integrated Data Loss Prevention
    d. Device Control
    e. Email Security for Google Workspace
    f. Web Reputation
    g. Ransomware Rollback
    h. Extended Detection and Response (XDR)

2. Server Security Licenses with the following features:
    a. Hosted Intrusion Detection System (HIPS)
        i. Virtual Patching
    b. Anti-Malware
    c. Hosted Firewall
    d. Integrity Monitoring
    e. Log Inspection
    f. Application Control

g. Web Reputation
h. Support for Windows, Linux and Solaris OS
i. Extended Detection and Response (XDR for Servers
j. With Yubikey

3. Managed Detection and Response Service with the following features:
   a. Managed XDR for Endpoint Security for endpoint, email and servers
   b. Managed XDR for Server Security for end point, email and servers
   c. Premium Support Services with dedicated Technical Account Manager

V. OBJECTIVES

To protect and secure all IT based assets which include servers, workstations, email, cloud-based storage and web access from software viruses, malware and anti-ransomware.

To effectively monitor and defend against cybersecurity threats of IT assets at all times via a 24 x 7 threat monitoring service which includes detection, response and remediation

VI. PROJECT STANDARDS AND REQUIREMENTS

A. ENDPOINT (WORKSTATION) SECURITY

- Coverage: 2,000 Licenses for one year

1. GENERAL FEATURES

- Complete laptop and desktop protection defends against everything from traditional attacks to the latest sophisticated targeted threats.
- The proposed solution must have cloud-based management.
- Cloud Based protection for 2000 workstation licenses inclusive of web reputation security, email security, and sandbox of the same brand with the server security solution
- Both virtual and physical endpoints are secured with multiple layers of anti-threat techniques uniquely adapted to each environment.
- Advanced threat protection includes, anti-malware, command and control blocking, browser exploit protection, application control, behavior monitoring, ransomware protection, memory inspection, email gateway protection, cloud email protection, web threat protection, and vulnerability protection.
- Application and port control make sure that your users don’t execute dangerous applications on your endpoints or send information where it doesn’t belong.
- Vulnerability protection shields against vulnerabilities even after end of support.
- Integrated, template-based data loss prevention ensures information is protected at the endpoint and across multiple layers.
- Light weight and optimized security ensure minimal impact on device, application, or network performance.
- Real-time connected threat intelligence correlates threat data across multiple

threat vectors from a global threat intelligence network

- The solution should be a leader in Gartner's Magic Quadrant for Endpoint Protection Platforms for 2021.
- The solution should be a Leader in The Forrester Wave: Endpoint Security Software as a Service: Q2, 2021
- The solution should be a leader in Forrester Wave: Endpoint Detection and Response, Q1 2021
- The solution should be part of the top 3 IDC Worldwide Corporate Endpoint Security Market Shares, 2021
- The proposed solution must be able to work with Microsoft Windows Security Center.
- The proposed endpoint and server security solution should support the following endpoint operating system

  Windows
    - Windows 7 32bit/64bit
    - Windows 8.1 32bit/64bit
    - Windows 10 32bit/64bit

  Macintosh
    - maCOS Catalina 10.15
    - maCOS Mojave 10.14
    - maCOS High Sierra 10.13
    - OD X EI Capitan 10.11

2. MANAGEMENT

- Should have a Centralized Management Console.
- Should be a Single, Configurable Installation with centralized configuration & solid management.
- The proposed solution must be manageable through Web browser.
- Should have logical group based on IP addresses (Subnets). Should support integration with Active directory for directory structure of computers for better management.
- The proposed solution must support role based for administrator account.
- The administrator users administrative access must be different from the role-based administrative access.
- The proposed solution must allow the administrator to customize the dashboard.
- The proposed solution must have audit logs for changing of policies.
- The proposed solution must have audit logs for every action done on the console (example issue of isolation command).
- The proposed solution must be able to recover the licenses from those endpoints that have not been connected to the management console within the defined period.
- The proposed solution must allow the administrator to upgrade agent from the management with no need of third-party tool.
- The proposed solution management shall have an actionable GUI that allow administrators to respond on the fly.
- The proposed solution must allow user to integrate with third-party Intelligence

(example Virus Total). The proposed solution must provide API for third party integration example SIEM, SOAR.

- The proposed solution must be able to manage Microsoft bitlocker disk execution.
- The proposed solution must be able to temporarily allow user to use their USB drives in the event of emergencies.

3. ANTI-VIRUS and ANTI-MALWARE

- Anti-malware (pattern-based and signature-less high-fidelity machine learning for pre-execution and runtime)
- The proposed solution shall have Behavioral Analytics (against scripts, injection, ransomware, memory and browser attacks).
- The proposed solution shall have File Reputation - Variant Protection - Census Check - Web Reputation The proposed solution shall have Exploit Prevention (host firewall, exploit protection.
- The proposed solution shall have Command and Control C&C -protection.
- Anti-Virus Software must have the capability to detect and clean Virus.
- The proposed solution shall provide common definitions for all Operating Systems supported & across all product ranges.
- The proposed solution shall be able to update definitions & scan engines on the fly, without a need for reboot or stopping of services on servers. Users should be prevented from being able to uninstall the anti-virus software.
- The MAC OS security solution can provide more that the regular antimalware protection. It should also include Capabilities such as device control, machine learning.
- The solution does not require a separate management console for MAC clients. Everything should be viewable and managed under a single pane of class.
- The security agent adheres to the Mac OS X look and feel for positive user experience.

4. THREAT PREVENTION and VULNERABILITY PROTECTION

- The solution is able to stop new or emerging threats that could potentially compromise your security regardless of the platform
- The solution is able to perform virtual patching for vulnerable operating systems
- The vulnerability protection solution is integrated on a single security agent
- The proposed solution must be able to prevent threats without signatures.
- The proposed solution must be able to prevent fileless malware.
- The proposed solution must be able to protect endpoint against Ransomware.
- The proposed solution must be able to protect endpoint against script attack.
- The proposed solution must allow user to customize Their prevention policy.
- The proposed solution must allow user to set restriction to application or processes.
- The proposed solution must allow user to define blacklist or whitelist processes by hash.
- The proposed solution must include static analysis technology, example like machine learning.
- The proposed solution must provide Malware prevention across Windows and MacOS.

- The proposed solution must be able to prevent suspicious files from executing from external media (example USB drive, CDROM)

5. DATA LOSS PREVENTION (DLP)

- The DLP solution provides visibility and control over sensitive data and prevent data loss via USB, email, software as a service application, web, and cloud storage. The DLP solution has built-in regional and industry-specific templates that complies with regional guidelines and regulations.
- The DLP solution should be integrated with the endpoint protection solution in a single agent.
- The DLP solution can detect and react to improper data usage-based keywords, regular expressions, and file attributes.
- The DLP solution can provide education to employees about corporate data usage policies through alerts, blocking or soft-blocking and reporting.
- The DLP solution has visibility and management over data at rest control - points.
- The DLP solution has visibility and management over data in motion control points.
- The DLP solution has visibility and management over data in use control points.

6. APPLICATION CONTROL

- The solution provides a capable allow or deny functionality that is able to manage known and unknown applications, file types, and executables
- The solution is able to provide a reliable file reputation source to allow cross checking of known good files. This source must be constantly kept up- to-date with the latest known good file listing
- The application control solution is integrated or can be integrated with other security solutions for better data correlation. It should complement security like antivirus, host intrusion prevention, data loss prevention, and mobile protection
- The solution is able to perform an automated inventory scan which categorizes installed applications depending on its file reputation - known good to potentially dangerous

7. EMAIL SECURITY

- The solution must support Gmail email service.
- The solution must have anti-virus, anti-spam and anti-relay protection.
- The solution must be able to quarantine emails upon virus detection.
- The solution must have heuristic anti-spam protection.
- The solution must be able to add policies based of custom references.
- The solution must be able to block/allow customized subjects based on keywords, etc. in any part of the email message.
- The solution must be able to support multiple domains.
- The solution must be able to protect against phishing websites.
- The solution must be able to block or approve senders list.
- The solution must have advanced detection and alert capabilities for early mitigation of emerging threats and targeted attacks.
- The solution must detect unknown URLs embedded in email messages.

- The solution must support protection against directory harvest attacks DHA.
- The solution must protect from malicious URLs embedded in email messages.
- The solution must have anti-spoofing feature. The solution must provide security for business email compromise (BEC).
- The solution must be able to capture and analyze all incoming emails from internet to Gmail mailboxes. The solution must be able to capture and analyze all outgoing emails from Gmail mailboxes to internet.
- The solution must be able to capture and analyze all Gmail internal email flows from Gmail mailbox to Gmail mailbox.
- The solution must support both real-time scans to protect data in motion and manual scan for data at rest.
- The solution must not impact or affect user email delivery or file sharing in case of service disruption or unavailability (pass-through).
- The solution must be able to prevent the delivery of an identified suspicious/threated email and files. The solution must be able to detect threats in emails without blocking the deliver to the recipient pass-through).
- The solution must meet data sovereignty requirement that data must stay at its own region.
- The solution must have SOC2-type 2 report for the management of the Cloud infrastructure.
- The solution must have 1S027001 certification for the management of security of the Cloud infrastructure.
- The solution must support business email (BEC) protection that includes writing style DNA technology to scan the English email messages of a desired individual to learn their Writing Style and generate a writing style mode.
- Should be a “Leader” in The Forrester Wave™: Enterprise Email Security, 2020 or 2021.

8. WEB PROTECTION

- The solution must have anti-virus and must be able to scan traffic ongoing in and out the network in real time.
- The solution must have URL database with multiple categories.
- The solution must be able to protect HTTP, FTP, SMTP, POP3 protocols.
- The solution must be able to create access policy by category, from URL database, customized list and by keyword.
- The solution must block forbidden internet application through a web browser.
- The solution must be able to block access to malicious sites and restricted areas.
- The solution shall be able to support scan HTTP and HTTPs traffic for spyware and another web threats.
- The solution shall be able to support blocking of outbound data to known spyware and Phishing-related websites.
- The solution must be able to validate web-based codes to screen web-based pages for malicious codes.
- The solution must be able to deploy policy based on Users and/or «roues defined in the active directory.
- The solution must be able to generate web security violations per use, hostname or IP.

- The solution must be able to generate reports on web violations statistics.

B. SERVER PROTECTION

- Coverage: 60 Licenses for one year

1. GENERAL FEATURES

- The solution must provide single platform for complete server protection over physical servers, virtual (server/desktop), & cloud servers in single management console.
- The solution must be of the same brand as the endpoint security and able to support hybrid datacenter, from on-premise servers to cloud servers, such as AWS, Microsoft Azure and the like
- The solution should meet 7 of 7 Recommendations in the 2020 Gartner Market Guide for Cloud Workload Protection Platforms.
- Provides layered defense against advanced attacks and shields against known and unknown vulnerabilities in web and enterprise application and operating systems.
- Web reputation prevents access to malicious web sites, domains, and IPs.
- The solution must provide layered defense against advanced attacks and shields against known and unknown vulnerabilities in web and enterprise applications and operating systems.
- The proposed solution provides self-defending servers; with multiple integrated modules below providing a line of defense at the server using a SINGLE AGENT:
    - Firewall
    - Intrusion Prevention (Virtual Patching, Web Application Protection IDS/IPS.
    - Web Reputation
    - Anti-Malware
    - Log Inspection
    - Integrity Monitoring
    - Application Control
- Protects a wide range of platforms which include Windows, Linux, Solaris, AIX, VMware, Citrix, Hyper-V, Amazon, Azure.
- The proposed solution should be able to support legacy operating systems such as Windows Server 2003
- The solution should be a leader in the The Forrester Wave™: Cloud. Workload Security, Q4 2020 or 2021.
- The solution must be compliant for FIPS 140-2 standard.
- The solution must be certified to Common Criteria EAL 2+
- The proposed solution should have Activity Monitoring for deletion and response support to provide complete visibility of the servers' activity.
- The activity monitoring feature should collect the following information from the servers.
    - Process activity
    - File activity
    - Network activity

- Connection activity
- Domain query activity
- Registry activity (Windows only)
- User account activity (Windows only)

2. SERVER ANTIMALWARE

- The proposed solution must be able to provide Web Reputation filtering to protect against malicious web sites
- Must have Predictive Machine Learning to protect against unknown malware
- Must have Behavioral Monitoring to protect against malicious script & applications.
- Must have Ransomware protection that can backup & restore encrypted documents.

3. HOST IPS FOR SERVERS

- Must be able to provide HIPS/HIDS feature
- Must feature a high-performance deep packet inspection engine that — examines all incoming and outgoing traffic for protocol deviations, content that signals an attack, or policy violations.
- Must be ABLE to operate in detection or prevention mode to protect operating systems and enterprise application vulnerabilities.
- Must provide detailed events with valuable information, including who attacked, when they attacked, and what they attempted to exploit. Administrators can be notified automatically via alerts when an incident has occurred must be able to provide protection against known and zero-day attacks.
- Includes out-of-the-box vulnerability protection for over 100 applications, including database, Web, email, and FTP services Must include smart rules to provide zero-day protection from unknown exploits that attack an unknown vulnerability, by detecting unusual protocol data containing malicious code.
- Must include exploit rules to stop known attacks and malware and are like traditional antivirus signatures in that they use signatures to identify and block individual, known exploits.
- Must include smart rules to provide zero-day protection from unknown exploits that attack an unknown vulnerability, by detecting unusual protocol data containing malicious code
- Must include exploit rules to stop known attacks and malware and are similar to traditional antivirus signatures in that they use signatures to identify and block individual, known exploits
- Must automatically shield newly discovered vulnerabilities within hours, pushing protection to large number of servers in minutes without as stem reboot.
- Must be able to provide Application Control on network layer.

4. HOST (SERVER) FIREWALL

- Must include an enterprise-grade, bidirectional stateful firewall providing centralized management of firewall policy, including predefined templates.
- Fine-grained filtering (IP and MAC addresses, ports).
- Coverage of all |P-based protocols (TCP, UDP, ICMP, GGP, \GI etc. and all

frame types (IP, ARP, etc.)
- Prevention of denial of service (DoS) attack.
- Design policies per network interface.
- Detection of reconnaissance scans.

5. INTEGRITY MONITORING

- Must be able to monitor critical operating system and application — files, such as directories, registry keys, and values, to detect and report malicious and unexpected changes in real-time.
- Provides integrity monitoring, extend security and compliance of virtualized systems. And must support Intel TPM/TXT technology.
- Provides File Integrity Monitoring and baseline or recommendation scan.

6. VIRTUAL PATCHING

- Provide virtual patching which shields vulnerable systems that are awaiting a security patch. Automatically shields vulnerable systems within hours and pushes out protection to thousands of VMs within minutes.
- Must have vulnerability rules to shield known vulnerabilities from an unlimited number of exploits. Automatically shields newly discovered vulnerabilities within hours.
- Must have the intelligence to provide recommended virtual patching rules to protect OS & Application.
- Must be able to create Scheduled Tasks to run recommendation scan to discover new rules to apply.
- Must be able to automatically assign new Virtual Patching rules through scheduled tasks.
- Must be able to automatically unassign Virtual Patching rules after physical patch has been installed.

7. LOG INSPECTION

- The proposed solution must be able to provide the capability to inspect logs & events generated by operating systems & applications.
- Able to automatically recommend and assign relevant log inspection rules to the server based on the operating system & applications installed.
- Able to automatically recommend and unassign log inspection rules that are not required.
- Proposed solution comes with predefined template for operating system and enterprise application to avoid manual creation of the rules.
- Proposed solution can create customized rule to support custom application.

8. APPLICATION CONTROL

- Able to monitor changes made to the server compared to baseline software.
- Able to allow or block the software and optionally lock down the server from unauthorized changes.
- Allows maintenance mode to allow installation of software and changes OS.
- Ability to manually input SHA-1 values to block specific files.

- Unauthorized scripts and applications should generate alerts in the console.

9. SUPPORTED PLATFORMS

Microsoft Windows

- Windows XP (32- and 64-bit)
- Windows Server 2003 R2 SP2 (32 and 64 bit)
- Windows Server 2008 R2 (32 and 64 bit)
- Windows Server 2012 R2 (32 and 64 bit).
- Windows server 2016 64bit
- Windows server 2019 64bit

Solaris

- Solaris OS 10 and 11

Linux

- RedHat Enterprise Linux 6, 7 and 8
- Ubuntu Linux 10,12, 14, 16, 18 and 20.04 (64-bit)
- SUSE Enterprise Linux 10, 11, 12 and 15 (32-bit/64-bit)
- Debian 8, 9 and 10
- CentosOS 6, 7 and 8 (32-bit/64-bit)

AIX

- AIX 6 and 7

C. EXTENDED DETECTION AND RESPONSE (XDR) SERVICE

- Coverage: 60 Server Licenses and 2,000 endpoint licenses including managed detection and response

1. PLATFORM GENERAL FEATURES

- The platform should have the capability to correlate events and integrate different security protection layers such as endpoint, email, server, and network in a single console of the same brand.
- The platform should have a security posture dashboard with customizable view to show alerts, attacks and reports
- The platform should provide investigation platform that provides view of possible tactic, techniques and procedures used by the attacker.
- The solution should have the capability to allow integration with 3rd party solutions via API.
- The platform should provide a view for easier response like endpoint isolation, collect files, search endpoint, check execution profile, quarantine the email or even block the email sender.
- The platform should be able to provide a preview of the critical users, machines and email accounts that needs prioritization for response.
- The platform should provide a platform where the administrator would have the latest view of the security breaches and info and links to the published articles.
- The platform should provide a platform for easier investigation like usual

graphical view and timeline of the attack.

- The platform must be able to Isolate at-risk endpoints to run an investigation and resolve security issues and then restore the connection promptly when all issues have been resolved.
- The platform must offer a built-in graphical triage viewer to ease security operations.

2. MANAGED DETECTION AND RESPONSE SERVICE

- The provider shall conduct 24 x 7 continuous alert monitoring, correlation and prioritization using automation and analytics, and provide proactive sweeping of endpoint, server, and email.
- The service shall include the following:
    - Monitoring and Detection
    - Analysis and Investigation
    - Response and Reporting
- The operations team of the provider shall be composed of internal employees (no outsourcing) of the manufacturer with expertise and rich experience within areas such as threat research, threat response and technical support. Security analysts should be based here in the Philippines
- The service and system shall determine alert severity as part of the initial analysis in order to filter and reduce the volume of alerts reviewed by the customer
- The provider shall evaluate the impact of the incident within the organization, Interpret the root cause chain, and determine threat profile, and perform advanced investigation
- The provider shall Initiate product response, provide remediation recommendations, create clean-up toolkits (if required), and monitor infection for reoccurrence
- The provider shall submit a monthly Executive Summary Report that contain alerts, events, investigations, response and recommendations
- Vendor platform should be ISO27001 certified and proof of certification should be provided
- The Engineer to be assigned must be a certified Global Information Assurance Certification (GIAC) Certified Incident Handler (GCIH)

3. PREMIUM SUPPORT SERVICE

- The Provider shall assign a dedicated Technical Account Manager to help leverage the deployed security solutions and optimize IT service levels
- The Technical Account Manager shall assist in the proactive security planning and provide consultancy service and assistance for crisis management planning
- The service shall include Security Planning twice a year
- The service shall include on-site support for emergency security incidents
- There should be 24 x 7 support and at least 4 hours' response time
- The service shall include remote problem diagnosis and remediation support, priority case handling, and proactive threat alerts
- The Technical Account Manager must be a certified Customer Success Manager and have project management skills and training

VII. DEPLOYMENT SERVICES and MAINTENANCE

- The Supplier shall provide the necessary test plans to ensure that all functional requirements are fully tested and sign off.
- The Supplier shall ensure the personnel carrying out the deployment shall be certified Professional vendor.
- The Supplier shall provide preventive maintenance every 12 months to ensure all software patches and configuration are up-to-date and operating optimally.
- The supplier must provide Security Health checks and Security Planning at least twice a year
- Training or equivalent for operational personnel administering the proposed solution shall be included for 5 personnel of the Quezon City Hall.
- Project Documentation shall be provided as follows:
    - Project Implementation Plan (include project schedule)
    - System Design (include architecture/setup description and design consideration)
    - User Acceptance Tests & Results Administrator and User Guide
    - Operational Maintenance & Support Guide (Includes: Technical Troubleshooting, FAQ, 1st Level Support Guide, Escalation Procedures
- The Supplier shall provide unlimited daily 24 by 7 phone and email support for problems encountered during operations.

VIII. ELIGIBILITY REQUIREMENTS

1. The bidder must be capable of implementing the project consistent with the primary purpose in its articles of incorporation approved by the SEC that it provides any and all acts that are associated with information and communication technology
2. Must be in the business of providing Information and Communication Technology products and services for at least five (5) years
3. The minimum work experience requirements for the key personnel are the following:
    - **a.** One (1) Certified Project Manager with at least five (5) years of experience in project management, design and implementation
    - **b.** Two (2) Post-sales / Implementation Engineer certified by the manufacturer with at least two (2) years' experience in cybersecurity technologies
    - **c.** Two (2) Threat Analysts with expertise and rich experience in threat research, threat response and technical support from the product manufacturer. The Engineer to be assigned must be a certified Global Information Assurance Certification (GIAC) Certified Forensic Analyst (GCFA) and/ ot certified Global Information Assusrance Certification (GIAC) Certified Threat Intelligence (GCTI) and/or Global Information Assurance Certification (GIAC) Certified Incident Handler (GCIH)
    - **d.** One (1) Technical Account Manager who shall provide proactive security planning and consultancy service for crisis management planning. The Technical Account Manager must be a certified Customer Success Manager and have project management skills and training

4. Certificate from the manufacturer indicating that the bidder is authorized to resell the product

IX. BUDGETARY REQUIREMENT

The approved budget cost of the contract/s for the Antivirus with Anti-Ransomware (Cloud based).

No.	ITEMS	QTY
1	**Endpoint Security**	**2,000.00**
	• Anti-Malware	
	• Application Control	
	• Integrated Data Loss Prevention	
	• Device Control	
	• Email Security for Google Workspace	
	• Web Reputation	
	• Ransome Rollback	
	• Extended Detection and Response (XDR)	
2	**Server Security**	**60**
	• Hosted Intrusion Detection System (HIPS)	
	- Virtual Patching	
	• Anti-Malware	
	• Hosted Firewall	
	• Integrity Monitoring	
	• Log Inspection	
	• Application Control	
	• Web Reputation	
	• Support for Windows, Linux and Solaris OS	
	• Extended Detection and Response (XDR) for Servers	
	• With Yubikey	
3	**Managed Detection and Response**	**2,060**
	• Managed XDR for Endpoint Security	
	• Managed XDR for Server Security	
	• Premium Support Services	
	Professional Services (included):	
	• Included one-time implementation and deployment of the following :	
	- 1 Apex One SaaS w/ XDR console configuration	
	• Includes HIPS configuration	
	• 2000 pilot Apex One SaaS Agents	
	- 1 Cloud One Workload Security w/ XDR console configuration	
	• 60 ClouD One Workload Security agents	
	- Knowledge Transfer	

	• 8x5 Support Services - Mondays through Fridays (except holidays)	
	* Additional services that are not stated above will be for further discussion, scoping and price revision.	
	*****nothing follows*****	

X. PROJECT DURATION

One-year protection. Renewable on an annual basis. Implementation must be completed within 120 days upon the issuance of Notice to Proceed (NTP)

XI. APPROVED BUDGET FOR THE CONTRACT

Source of Fund:	**General Fund**
The Approved Budget for the Contract is:	**P 12,743,320.98**

XII. BASIS OF PAYMENTS

One-time payment upon delivery of the licenses agreement inclusive of license codes, serial numbers and/ other related documents.

XIII. PENALTIES FOR BREACH OF CONTRACT

Failure to deliver the services according to the standards and requirements set by the City shall constitute an offence and shall subject the Contractor to penalties and/or liquidated damages pursuant to RA 9184 and its revised Implementing Rules and Regulations.

.

XV. CANCELLATION OR TERMINATION OF CONTRACT

Should there be any dispute, controversy or difference between the parties arising out of this TOR, the parties herein shall exert efforts to amicably settle such dispute or difference. However, if any dispute, controversy or difference cannot be resolved by them amicably to the mutual satisfaction of the parties, then the matter may be submitted for arbitration in accordance with existing laws, without prejudice for the aggrieved party to seek redress before a court of competent jurisdiction.

The guidelines contained in RA 9184 and its revised IRR shall be followed in the termination of any service contract. In the event the City terminated the Contract due to default insolvency, or for cause, it may enter into negotiated procurement pursuant to section 53(d) of RA 9184 and its IRR.

PREPARED BY:

JUANCHO C. DEL MUNDO
ITO III – PRDD

APPROVED BY:

PAUL RENE S. PADILLA
HEAD, ITDD