TOURISM PROMOTIONS BOARD PHILIPPINES

TECHNICAL SPECIFICATIONS
Service Provider for the Subscription-Renewal of Business Antivirus

1. BACKGROUND

Since its establishment in 2008, Endpoint Security Application has been at the forefront of cybersecurity, providing advanced antivirus and anti-malware solutions to protect against a wide range of online threats. At TPB, we have been using Malwarebytes to safeguard our systems from malware, viruses, ransomware, and phishing attacks. The software's real-time protection, advanced threat detection, and comprehensive scanning capabilities ensure our network remains secure and free from malicious activities. The Endpoint Security Application's user-friendly interface and centralized management also simplify maintaining robust security.

The solution has significantly improved TPB's network management capabilities by reducing unnecessary bandwidth consumption, strengthening security protocols, and providing valuable insights into internet usage, leading to enhanced productivity and better resource allocation.

2. OBJECTIVES

2.1. **Ensure Continuous Protection:** To safeguard TPB's network and data and maintain continuous, up-to-date protection against evolving cyber threats.

2.2. **Enhance Threat Detection and Prevention**: Utilize advanced threat detection and real-time protection capabilities to prevent malware, viruses, ransomware, and phishing attacks.

2.3. **Improve Security Management**: Streamline security management through a user-friendly interface and centralized dashboard, enabling efficient monitoring and control of all devices within the organization.

2.4. **Maintain Compliance and Standards**: Adhere to industry standards and regulatory compliance requirements by ensuring robust cybersecurity measures are in place with Malwarebytes' protection.

2.5. **Support IT Efficiency**: Leverage Malwarebytes' comprehensive scanning and threat removal tools to enhance the IT department's efficiency, allowing the team to focus on other critical tasks.

2.6. **Protect Sensitive Data**: Safeguard TPB's sensitive data from unauthorized access and potential breaches through advanced security features and regular updates provided by Malwarebytes.

3. SCOPE OF WORK/SERVICES/DELIVERABLES

Supply, delivery, and configuration of Business Anti-Virus License to wit:

License	Qty	Subscription	ABC (in PHP)
Business Anti-Virus (Endpoint Protection, Vulnerability Assessment, Application Block)	250	12 Months	1,000,000.00
Mobile Security for Business (Endpoint Protection for iOS, Android, and Chrome devices)	15	12 Months	Free

4. PROJECT TIMELINE

Must be delivered on or before 11 October 2024, after which liquidated damages shall be imposed. The subscription shall be effective for one (1) year from the commencement date.

5. MINIMUM REQUIRED TECHNICAL SPECIFICATIONS

BUSINESS ANTIVIRUS

5.1. **OPERATING PLATFORM:**

- 5.1.1. Windows
- 5.1.2. Mac
- 5.1.3. iOS
- 5.1.4. Android
- 5.1.5. Chrome

5.2. **CORE FEATURES:**

- 5.2.1. Cloud management console
- 5.2.2. Includes next-gen antivirus software
- 5.2.3. Real-time protection against malware and other threats
- 5.2.4. Ransomware, zero-day exploits, phishing protection
- 5.2.5. Brute force RDP, file-less protection
- 5.2.6. Best-in-class threat remediation
- 5.2.7. Single, lightweight agent
- 5.2.8. Automated, on-demand reports
- 5.2.9. Optional server security

5.2.10. Threat hunting, isolation, recovery
5.2.11. Windows ransomware rollback
5.2.12. Priority phone support
5.2.13. Optional premium support
5.2.14. Endpoint Protection
5.2.15. Vulnerability Assessment
5.2.16. Application Block
5.2.17. Incident Response

5.3. **THREAT REMEDIATION:**
5.3.1. Cleans infected devices
5.3.2. On-demand and scheduled threat scans
5.3.3. Comprehensive malware/artifact removal
5.3.4. Non-persistent/Dissolvable remediation agent
5.3.5. Isolates detected threats for later remediation
5.3.6. Forensics tools for Windows environments
5.3.7. Unmanaged endpoint discovery and agent deployment

5.4. **THREAT PREVENTION:**
5.4.1. Real-time Viruses, malware, spyware protection
5.4.2. Real-time Ransomware protection
5.4.3. Zero-day, file-less attack protection
5.4.4. Stops brute force remote desktop protocol (RDP) attacks

5.5. **MULTI-VECTOR PROTECTION:**
5.5.1. Web Protection – Helps prevent access to malicious websites, ad networks, scammer network
5.5.2. Application Hardening – Reduces vulnerability exploit surface and proactively detects fingerprinting attempts used by advanced attacks
5.5.3. Exploit Mitigation – Proactive detects and blocks attempts to abuse vulnerabilities and remotely execute code on the endpoint
5.5.4. Application Behavior Protection – Helps prevent applications from being leveraged to infect the endpoint
5.5.5. Anomaly Detection Machine Learning – Proactive identifies unknown viruses and malware via machine learning techniques
5.5.6. Payload Analysis – Anti-malware technology that identifies entire families of known and relevant malware with heuristic and behavior rules
5.5.7. Ransomware Mitigation – Detects and blocks ransomware via behavioral monitoring technology

5.6. **MANAGEMENT:**
5.6.1. Centralized management console
5.6.2. Threat visibility dashboard
5.6.3. Asset Management – Collects and displays endpoint details, including

installed software, updates, startup programs, and more

5.6.4. Automated and on-demand reports
5.6.5. Email notifications, Syslog support
5.6.6. Role-based access control (RBAC)
5.6.7. Tamper Protection
5.6.8. Single sign-on with SAML 2.0 support
5.6.9. Active Directory integration
5.6.10. Integration with existing security and management tools

5.7. **SUPPORT:**

5.7.1. Email, chat, remote technical support
5.7.2. 24/7 - Phone technical support

6. APPROVED BUDGET FOR THE CONTRACT (ABC):

6.1. One Million Pesos only (Php 1,000,000.00)
6.2. Inclusive of all applicable fees and taxes

7. BIDDER REQUIREMENTS:

7.1. Must be an ICT Company operating for at least five (5) years, experienced in dealing with different government offices and private companies.
7.2. Must provide a Reseller Certificate for the proposed product.
7.3. Must provide brochures or images of the proposed product.

8. PAYMENT TERMS AND SCHEDULE:

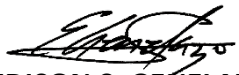
Payment will be made via a send-bill arrangement and settled within thirty (30) calendar days of receipt of the statement's billing.

Payments will be made through a Landbank of the Philippines (LPB) deposit. If the supplier does not have an LBP account, the supplier will shoulder bank charges.

9. PROJECT OFFICER AND ALTERNATE PROJECT OFFICER:

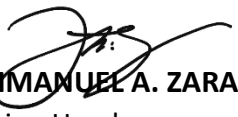
Name	Edison S. Genelazo Ian Santos
Email Address	edison_genelazo@tpb.gov.ph ian_santos@tpb.gov.ph
Landline #	8-5259318 to 27 Loc. 215

Prepared by:



EDISON S. GENELAZO
Computer Maintenance Technologist II
Date: _____

Noted by:



EMMANUEL A. ZARATE
Acting Head
Management Information Systems Department
Date: _____