



Republic of the Philippines

**DEPARTMENT OF SCIENCE AND
TECHNOLOGY**

**Philippine Atmospheric, Geophysical and Astronomical Services
Administration (PAGASA)**

**TERMS OF REFERENCE
FOR THE SUPPLY, DELIVERY AND INSTALLATION OF
FORTIMAIL SOFTWARE UPDATE AND SUPPORT FOR ONE YEAR**

A. BACKGROUND

Aside from telephone, fax and social media, PAGASA is utilizing EMAIL services in disseminating weather information to general public, disaster managers, inter-government agencies, and other local and international meteorological channels.

Email service is a prime target for attackers and disruptors. Hackers find email as the easy medium to spread malware by sending deceptive spam emails, most oftentimes attached with virus-infected files to unwary recipients. Another attack is flooding the mail server with hundreds of thousands of spam mails causing the mail server to be temporarily down, thus disrupting the email services operation. Methods of attacking email are continuously advancing, more sophisticated and more dangerous. With the alarming rise of constant evolution of cyber-attacks, implementing multiple security measures to enhance email security is a must.

The current Fortimail security gateway, as first line of defense, is protecting the PAGASA email server from an increasing number of inbound malwares, spam, phishing, malicious attachment and ransomware attacks. Unfortunately, the software update and support will cease to operate in January 2023 thus will affect several security functions. It is very essential to renew the software update and support at least for one year to continuously protect the email communication services.

B. APPROVED BUDGET FOR THE CONTRACT (ABC)

The Approved Budget for the Contract is **NINE HUNDRED SIXTY THOUSAND PESOS (Php 960,000.00)** inclusive of VAT and all applicable government taxes.

C. PLACE AND DATE OF DELIVERY

The winning bidder shall supply and deliver the deliverables at PAGASA WFFC building within thirty (30 c.d.) calendar days from receipt of the Notice to Proceed (NTP).

D. LIST OF DELIVERABLES

- Installation of Fortimail software update and one-year maintenance support warranty.
- Setup, configuration and customization of existing Fortimail email security gateway including integration of offered appliance to the existing email server.

E. TECHNICAL SPECIFICATIONS

1) SOFTWARE UPDATE MAIN FEATURES

- a) With range of deployment options:
 - Transparent, Gateway and Server Mode
- b) Inbound and Outbound Inspection
- c) Support for multiple email domains with per-domain customization:
 - MSSP multi-tenant support with white label support
 - Multi-tier administration
- d) IPv4 and IPv6 Address Support
- e) Virtual Hosting using Source and/or Destination IP Address Pools
- f) SMTP Authentication via LDAP, RADIUS, POP3 & IMAP LDAP-Based Email Routing
- g) Per User Inspection using LDAP Attributes on a Per Policy (Domain) Basis
- h) Comprehensive Webmail Interface for Server Mode Deployments and Quarantine Management
- i) Mail Queue Management
- j) Multiple Language Support for Webmail and Admin Interface
- k) SMTP RFC Compliance
- l) Modern HTML 5 GUI
- m) Independently tested by VBSpam, NSS, ICSA, SELabs
- n) Compatibility with cloud services e.g., Office365, Google G-Suite

2) ANTI-SPAM SERVICE

- a) Antispam service
 - Global sender reputation
 - Spam object checksums
 - Dynamic Heuristic Rules
- b) Real-time spam outbreak protection
- c) URL Category Filtering includes:
 - Spam, malware and phishing URLs
 - Newly registered domains
- d) Business Email Compromise (BEC):
 - Multi-level Anti-spoof protection
 - Impersonation analysis greylisting for IPv4/IPv6 add. & Email accounts
- e) Local sender reputation (IPv4, IPv6 and End Point ID-based)
- f) Behavioral analysis
- g) Deep email header inspection
- h) Integration with third-party spam URI and real-time blacklists (SURBL/RBL)
- i) Newsletter (greymail) and suspicious newsletter detection
- j) Block/safe lists at global, domain, and user levels
- k) Support for enterprise sender identity standards:
 - Sender Policy Framework (SPF)
 - Domain Keys Identified Mail (DKIM)
 - Domain-Based Message Authentication (DMARC)

- l) Flexible action and notification profiles
- m) Multiple system and per-user self-service quarantines

3) ANTI-MALWARE SERVICE

- a) Antivirus detection:
 - CPRL signature checking
 - Heuristic based behavioral detection
 - Greyware detection
- b) Virus Outbreak protection:
 - Global threat intelligence and data analytics
- c) Active content detection (PDF & Office Documents)
- d) Rescan for threats on quarantine release
- e) Custom file hash checking

4) TARGETTED ATTACK PROTECTION

- a) Content Disarm and Neutralization:
 - Neutralize Office and PDF documents (remove macros, active content, attachments and more)
 - Neutralize email HTML content
 - Remove URL hyperlinking and Rewrite URLs
- b) URL Click Protect to rewrite URLs and rescan on access
- c) Impersonation analysis: manual and automatic address impersonation detection
- d) Cloud and On-premise sandbox integration supporting file and URL analysis.

5) CONTENT DETECTION AND PROTECTION

- a) Mime and file type detection
- b) Comprehensive data-loss prevention with file fingerprinting and sensitive data detection:
 - Automatic Windows fileshare and manual upload file fingerprinting
 - Personally identifiable information and profanity detection
- c) Automatic decryption of Archives, PDF and Office Documents using built-in and administrator-defined password lists and word detection within email body
- d) PDF Scanning and image analysis Dynamic Adult Image Analysis Service:
 - Identify and report or block the transmission of adult content.

6) ADVANCED FEATURES

- a) Policy-based e-mail archiving with remote storage options:
 - Support for Exchange journal archiving
- b) Comprehensive encryption support:
 - Server to server TLS
 - Clientless Identity-based Encryption
 - S/MIME
- c) Advanced Email Server feature set including:
 - Comprehensive webmail interface
 - POP3(S), IMAP(S) mail access

- Calendaring functions
- Undo Send
- d) SAML 2.0 SSO and ADFS integration for webmail and quarantine access
- e) Advanced MSSP feature set:
 - System wide rebranding
 - Multi-tenancy and mass provisioning
 - Delegated tiered administration and role-based control.

F. MAINTENANCE SUPPORT WARRANTY

During the 1-year warranty period, the winning bidder shall provide software updates and maintenance support services warranty which shall include the following:

- 1) Warranty period starts from the date of acceptance.
- 2) Regular software updates, daily virus patterns, mail security, and firmware updates within the one-year subscription period.
- 3) Availability of Technical Support services via telephone, text, and email which include Remote Access Assistance thru Internet web or VPN access.