Technical Specifications

Procurement for the Renewal of Email Management Licenses and Office Suite Subscription for the Department of Foreign Affairs

Approved Budget for the Contract (ABC): PHP 40,738,000.00

I.	**Background**
	The Department of Foreign Affairs, hereinafter referred to as the DFA, requires the renewal of its Email Management licences and Office Suite Subscription to maintain uninterrupted communication, collaboration, as well as productivity among the DFA officials and employees across the Home Office, Foreign Service Posts, and Consular Offices. This renewal is essential to support daily operations, facilitate seamless coordination across the offices and enhance delivery of quality services to the general public.
II.	**Objective**
	The DFA aims to renew its email management licenses and office suite subscription from a reliable provider offering comprehensive email licenses and integrated collaboration tools. The renewal shall be implemented throughout the DFA to enhance the efficiency, security, and functionality of communication among personnel in the Home Office, Foreign Service Posts, and Consular Offices. By renewing these services, the DFA aims to: 1. Maintain uninterrupted and secure communication among officials, employees. 2. Enhance collaboration and productivity through cloud-based applications. 3. Support the department's digital operations in line with its mandate to provide effective and efficient services to the public. 4. Ensure data security and compliance with government policies and international standards. 5. Minimize operational disruptions by renewing existing services without delays or compatibility issues.

III.	**Scope of Work**	**Compliance**
	The Contractor shall provide a one (1) year subscription for a minimum total of Four Thousand Five Hundred (4,500) licenses that integrate seamlessly with the Department's existing email service. After allocating the specified number of licenses for the other license types below, the remaining number of licenses should be allocated for Enterprise Starter Licenses. 1. **Enterprise Starter licenses:** Each account will have at least 1TB of secure, cloud-based file storage. Features include a shared drive, fundamental Mobile Device Management (MDM), Data Loss Prevention (DLP) reports, basic audit logs, and Data Region Lite. **2. Thirty (30) Enterprise Standard licenses:** Each account will have at least 5TB of secure, cloud-based file storage. In addition to the features of the Enterprise Starter licenses, these licenses support video conferences for up to 500 participants (with up to 10,000 viewers) and include AI-powered noise cancellation. 3. **Twenty (20) Enterprise Plus licenses:** Each account will have at least 5TB of secure, cloud-based file storage. These licenses include all features of the Enterprise Standard licenses, plus video conferencing for up to 500 participants (with up to 100,000 viewers), AI noise cancellation, Vault, advanced Data Loss Prevention, Cloud Identity Premium, advanced enterprise control and customization, Cloud Search, AppSheet Core, Connected Sheets, and integration with third-party archiving tools. 4. **Three Hundred (300) Business Starter licenses:** Each account provides at least 30GB of cloud storage for documents, emails, and files. Features include a meeting platform with Meet rooms, background blur, whiteboarding, and live captions. 5. Mailboxes and Storage Accounts shall be transferable.	
IV.	**Technical Specifications**	
	Enterprise Starter licenses:	
	Store and back up files securely in the cloud with at least 1 TB of pooled storage per user.	

	Join secure video meetings from laptop or other device (up to 250 participants).	
	With a Meeting platform compatible with the existing system, equipped with moderation controls, hand raising, polling and Q&A, breakout rooms, noise cancellation and attendance tracking.	
	With meeting recordings saved to cloud storage used by the existing system.	
	Share calendars to easily schedule meetings and events	
	Collaborate in real-time on online documents, spreadsheets, and presentations	
	Manage user accounts and security settings from a central Admin console	
	Enterprise Standard licenses:	
	Store and back up files securely in the cloud with at least 5 TB of pooled storage per user, with the option to purchase additional storage as required, subject to an additional fee.	
	Join secure video meetings from laptop or other device (up to 500 participants).	
	Capable of full recording of online meetings	
	With in-call digital whiteboarding, polling, Q&A, hand rising and breakout rooms	
	With Advanced Data Loss Prevention for emails and cloud-based storage.	
	Enterprise Plus licenses:	
	Store and back up files securely in the cloud with at least 5 TB of pooled storage per user, with the option to purchase additional storage as required, subject to an additional fee.	
	Security, Premium administrative controls and Enterprise-wide collaboration	
	Enhance security of the cloud storage used by the existing system and electronic mail platform compatible with the existing system with data loss prevention (DLP). Scan for sensitive	

	information, such as credit card or Social Security numbers, and prevent sharing.	
	Protect the Department with security analytics, best practice recommendations, and the ability to remediate security incidents with the security center.	
	Set up rules to detect harmful attachments in a virtual environment using the Security Sandbox.	
	Ability to connect LDAP-based applications and services to Cloud Identity or Google Workspace, which is the current system being used, with Secure LDAP.	
	Manage company owned mobile devices using Apple Business Manager and Android Zero Touch.	
	Use enhanced desktop security for Windows to remotely apply Windows settings and manage users' devices.	
	Create granular access control policies to Google Workspace, which is the current system being used, and SAML applications based on attributes such as user identity, device security posture, IP address, and geolocation with context-aware access.	
	Scan images for text to identify and mitigate loss of confidential data in scanned images.	
	Able to use a third-party archiving product to store and discover mission-critical email.	
	Analyze e-mail logs in the current system being used in BigQuery using advanced and customized queries.	
	Automate mobile management tasks by setting custom rules that get triggered by suspicious events.	
	Automate user provisioning, authorize apps, and set rules for mobile management with Cloud Identity Premium.	
	Set up enterprise-grade meetings with up to 250 participants and live streaming.	
	Record and share online meeting sessions in the current cloud storage being used.	

	Analyze, visualize, and share data from spreadsheet with Connected Sheets.	
	AppSheet—ICT Personnel in the Department can build applications without coding.	
	Storage and Archiving Specifications	
	Each Storage account shall be capable of:	
	1. Archiving, e-discovery and information management capabilities;	
	2. Defining retention policies that are automatically applied to email and chat messages;	
	3. Archiving of email and chat messages according to email system policies defined by the user preventing inadvertent deletions; and	
	4. Running reports on user activity and actions in the archive wherein searches, message views and exports are shown.	
	Business Starter licenses:	
	Store and back up files securely in the cloud with 30 GB pooled storage per user (pooled).	
	Join secure video meetings from laptop or other device (up to 100 participants).	
	Share calendars to easily schedule meetings and events.	
	Collaborate in real time on online documents, spreadsheets, and presentations.	
	Communicate in groups or one-on-one, with text and rich media.	
	Mailbox Specifications	
	Each Mailbox account shall:	
	1. Maintain @dfa.gov.ph (DFA's official domain name).	
	2. Provide anti-spam and anti-malware functions for all incoming emails and provide anti-malware function for all outgoing emails;	

	3. Provide Information Rights Management (IRM), Transport Layer Security (TLS) enforcement, Phishing prevention;	
	4. Support verification of Sender Policy Framework (SPF) protocol for authenticity purpose and Simple Mail Transfer Protocol over Transport Layer Security (SMTP over TLS) protocol for secure transmission encryption;	
	5. Provide two-factor authentication composed of but not limited to password requirement and SMS verification code;	
	6. Comply with the following international operations standard and controls: a) ISO 27001 (Information security management), b) ISO 27017 (Security controls for cloud services), c) ISO 27018 (Cloud privacy protection overview), d) Service Organization Control (SOC) 2	
	7. Send and receive emails with attachments of different file types including but not limited to video, audio and image files;	
	8. Provide Office document creation, sharing and collaboration, offline/online editing, import and export of data files, revision/versioning through a browser;	
	9. Search, through Optical Character Recognition (OCR) and image recognition;	
	10. Create electronic forms to conduct survey and questionnaire online;	
	11. Provide an online social platform for information sharing and employee engagement;	
	12. Allow transfer from one service provider to another without loss of current data;	
	13. Be accessed through Android, iOS, Windows Phone, and Blackberry devices, Windows, MacOS desktops, laptops and tablets;	
	14. Have a cloud-based platform which can be accessed through popular web browsers including, but not limited to, Chrome, Firefox, Safari, Internet Explorer 11 and Edge;	
	15. Be accessed through Internet, Local Area Network (LAN), Wi-Fi, and hotspot environment by mobile devices;	
	16. Provide instant messaging and video conferencing (audio, video) through LAN, internet, Wi-Fi, and hotspots;	

	17. Provide shareable calendar services among users and guests;	
	18. Adopt current IT network setup and settings, and no new hardware/software requirements are needed to avail of the service;	
	19. Provide Mobile Device Management (MDM) and policy-based browser security management;	
	20. Be accessed 24x7, 365 days a year, at least 99.9% monthly uptime guarantee of the services;	
	21. Setup disaster recovery plans and secured back-up facilities or disaster proof facility to provide uninterrupted service; and	
	22. Customize, relative to DFA's requirements, user-friendly menus (mailbox organization).	
IV.	**Contractor's Responsibility**	
	The Contractor shall provide the following:	
	1. 24 x 7 technical support through telephone, email and/or chat with a maximum response time of two (2) hours from the posting/submission of support request;	
	2. Initial setup and configuration services for the DFA and shall ensure that proposed mail domain (*@dfa.gov.ph) is functioning normally.	
V.	**Contractor's Eligibility**	
	1. The Contractor shall present Certificates and/or Authorization to represent Original Product Manufacturer or proof of Authority for Distributorship, or Re-seller Dealership.	
	2. The contractor shall provide Professional Workspace Administrator Certificate/s or its equivalent.	
	3. The certificate holder/s must be a regular employee of the contractor as evidenced by the holder/s' Certificate of Employment, and Company Identification.	
	4. The contractor shall provide the most recent Certificate of Partnership with the Original Product Manufacturer and it must be Premier Level.	

VI.	**Duration**	
	1. The Contractor shall provide the email subscription and corresponding support applications for the DFA for a period of twelve (12) months.	
VII.	**Delivery**	
	1. The Contractor shall provide and activate the accounts within 7 working days upon receipt of Notice to Proceed (NTP).	
VIII.	**Confidentiality**	
	1. The Contractor shall ensure that each of its personnel assigned to provide support service executes and signs a Non-Disclosure Agreement which is to be submitted to the Department prior to commencement of the service. 2. The Contractor shall not disclose any confidential information accessed through the use of its services in relation to the official functions or operations of the Department without prior consent from the latter. 3. The Contractor shall immediately inform the Department of breaches, attacks, or other forms of cyber threats/activities that may contribute to disclosure of any confidential information. 4. Failure to comply with the confidentiality clause shall be subject to penalties as provided in Republic Act No. 10173 – Data Privacy Act of 2012 and all other relevant rules and regulations.	
IX.	**Payment**	
	1. The payment shall be made within thirty (30) working days upon full implementation of the system and receipt of the invoice with complete requirements through List of Due and Demandable Accounts Payable (LDDAP).	
	2. All payments shall be inclusive of all applicable taxes and other lawful charges.	

Note:

Bidder must state compliance to each of the provisions in the Terms of Reference/Technical Specifications, as well as to the Schedule to Requirements. The **STATEMENT OF COMPLIANCE** must be signed by the authorized representative of the Bidder, with proof of authority to sign and submit the bid for and in behalf of the Bidder concerned. If the Bidder is a joint venture, the

representative must have authority to sign for and in behalf of the partners to the joint venture. All documentary requirements should be submitted on or before the deadline for the submission of bids.

Bidders must state here either “Comply” or “Not Comply” against each of the individual parameters of each Specification stating the corresponding performance parameter of the equipment offered. Statements of “Comply” or “Not Comply” must be supported by evidence in a Bidders Bid and cross-referenced to that evidence. Evidence shall be in the form of a manufacturer’s un-amended sales literature, unconditional statements of specification and compliance issued by the manufacturer, samples, independent test data etc., as appropriate. A statement that is not supported by evidence is subsequently found to be contradicted by the evidence presented will render the Bid under evaluation liable for rejection. A statement either in the Bidders statement of compliance or the supporting evidence that is found to be false either during Bid evaluation, post-qualification or the execution of the Contract may be regarded as fraudulent and render the Bidder or supplier liable for prosecution subject to the provisions of **ITB** Clause 3.1 (a)(ii) and/or **GCC** Clause 2.1 (a)(ii)

Conformé:
[Signature/s]
[Name of Bidder’s Authorized Representative/s]
[Position]
[Date]